

# Abercrombie Primary School

## Online Safety Policy

## Contents of Online Safety Policy:

1. Introduction
2. Context and background
3. Roles and Responsibilities
4. Technical and Hardware Guidance
5. Online Safety for pupils
  - a. Internet access at school
  - b. Using the Internet for learning
  - c. Teaching the safe use of the Internet
  - d. Using email with pupils
  - e. Chat and online discussions
  - f. Other online technologies – mobile phones etc
  - g. Cyber Bullying
  - h. Contact Details and Privacy
  - i. Deliberate misuse – procedures and sanctions
  - j. Complaints
  - k. Online Safety Class Rules for KS1 and KS2
6. Use of ICT by school staff (Acceptable Use)
7. Data Protection policy
8. ICT Loans to staff – agreement form

# 1. Introduction

Our Online Safety Policy has been written by Abercrombie Primary School.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Created by: Charlotte Harris

Revised by Aaron Himsworth: March 2018

To be revised: March 2019

## 2. Context and Background

### **The technologies**

ICT in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

The Internet – World Wide Web (accessed through handheld devices and desktop computers)

Email

Instant messaging (often using simple web cams e.g. Instant Messenger) Web based voice and video calling (e.g. Skype, FaceTime)

Online chat rooms (via applications)

Online discussion forums and comment threads

Social networking sites and applications (e.g. Facebook, Twitter, Instagram, WhatsApp, Snapchat, Musical.ly, YouTube)

Podcasting (radio / audio broadcasts downloaded to computer or devices)

Music and video downloading (e.g. iTunes)

Smart phones/ tablets with e-mail, messaging, applications and internet access

### **Our whole school approach to the safe use of ICT**

Creating a safe ICT learning environment includes three main elements at this school:

An effective range of technological tools;

Policies and procedures, with clear roles and responsibilities

Online Safety teaching is embedded into safeguarding in the school curriculum and schemes of work.

### 3. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

#### **Leadership team**

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures

#### **Online Safety Co-ordinator**

Our school e-Safety Co-ordinator is Aaron Himsworth.

He is responsible for keeping up to date on all Online Safety issues and ensuring that staff are updated as necessary.

#### **Governors**

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

#### **School Staff**

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Staff should ensure they are familiar with the school Online Safety policy, and ask for clarification where needed.

They should sign the Staff Acceptable Internet Use agreement annually

Class teachers should ensure that pupils are aware of the Online Safety rules and advice, introducing them at the beginning of each new school year and spending some time exploring issues on the *Safer Internet Day* each spring.

#### **Pupils**

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with Online Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school.

#### **Parents**

Parents are given information about the school's Online Safety policy at the Admission interview. They are given copies of the support documents for information. They are also given the IT Code of Practice for Pupils and Parents/Carers and are asked to sign these along with their child and to support these rules with their children.

## 4. Technical and hardware guidance

### **School Internet provision**

The school used the standard LA Internet Service Provider, which is RM. RM also provides our internet filtering service.

### **Content filter**

Our Internet Provider uses a sophisticated content filter to ensure that, as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.

Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

### **Downloading files and applications**

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

### **Portable storage media**

Staff are allowed to use their own portable media storage (USB Keys etc). If use of such a device results in an anti-virus message, they should remove the device and immediately report to the ICT technician.

### **Security and virus protection**

The school subscribes to Sophos Antivirus software. The software is monitored and updated regularly by the school technical support staff

Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT technician.

## 5. Online Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in today's world, and ICT is an integral part of that world. At our school, we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

### Internet access at school

#### **Use of the Internet by pupils**

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

#### **Access for all pupils**

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, where this will directly support their learning.

We use various websites, with pupil logins, during the school day and encourage children and parents to login in to these at home too, to complete tasks and homework.

Some of these platforms are:

- My Maths (for maths homework)
- Purple Mash (Computing and curriculum wide tools for learning)
- Times Tables Rock Stars
- Discovery Education (Wider curriculum tool)

#### **Out of Hours Provision**

There is a breakfast club that runs each day from 7.45 – 8.45am and an afterschool club that runs from 3.30-5.45.

There will supervised access to the Internet during Out of Hours provision, and access to the internet will be limited and closely monitored, often used to facilitate online homework and projects.

### Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching new information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014)

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.

Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas, where necessary.

They are taught how to recognise the possible authors of web-based materials and carry out simple checks for bias and misinformation.

They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

## Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES <http://www.kidsmart.org.uk>

The main aspects of this approach include the following five **SMART** tips:

**Safe** - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...

**Meeting** someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...

**Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...

**Remember** someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...

**Tell** your parent or carer if someone or something makes you feel uncomfortable or worried...

### **Suitable material**

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

### **Non-Education materials**

We believe it is better to support children in finding their way around the Internet with guidance and positive role modeling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child -oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home. There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

### **Unsuitable material**

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident – ICT Incident Log Book in the school office
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future.

## Using Email at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

We teach the use of e-mail as part of our Computing curriculum, and use email accounts within the Purple Mash website.

Pupils are not allowed to access personal e-mail using school Internet facilities.

## Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered out, as part of the LA Internet policy

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

## Internet-enabled mobile phones and handheld devices

More and more young people have access to new internet-enabled devices such as Smartphones, tablets and other devices.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or blog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

## Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, sexting, email and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

No access to public chat rooms, Instant Messaging services and bulletin boards. Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

## Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

## School and pupil websites – pictures and pupil input

As part of the Computing and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work published on a public website and attributed to members of our school community, will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc., then identifying information will be removed, and images restricted.

## Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom and the Computer Room.

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

### **Unsuitable material (e.g. online games, celebrity pictures, downloads, sport websites etc)**

Initial warning from class teacher

Banning from Internet facilities

Report to Headteacher

Letter to parent/carer

### **Offensive material**

Meeting with Parent/Carer to re-sign Internet use agreement

Removal of access to Internet

Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

## How will complaints regarding e-Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

With international scale and the 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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

All incidents will be recorded

Interview/counselling by class teacher, Senior Management Team, Online Safety Coordinator and Headteacher;

Informing parents or carers;

Removal of Internet or computer access for a period

Referral to LA / Police.

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

## 6. Use of the Internet and ICT resources by school staff

*See Acceptable Use of Internet Policy for parents and children*

### Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

## 7. Data Protection Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

## 8. Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this Online Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Abercrombie Primary School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage.

They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'School Laptop Equipment and Software Loans Agreement' before taking the equipment away from the school premises.





