Aberford C of E Primary School

Acceptable Use Policy (AUP)

2020 - 2023

Online Safety Policy –

Internet Use in School

In conjunction with our Safeguarding & Child Protection policy, Safer Working Practice, AUP Policy, Data Protection Policy and Online Safety Policy

Adopted by Aberford C of E Primary School Governing Body in

Reviewed June 2020

To be reviewed by Governors in June 2023

Updated May 2020 in response to COVID-19

Introduction

At Aberford C of E Primary School, we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

This document sets out the policy and practices for the safe and effective use of the Internet at Aberford C of E Primary School. The policy has been drawn up in conjunction with the Data Protection Policy, Social Media Policy and the school's safeguarding and child protection policies and procedures.

The policy and its implementation will be reviewed regularly.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on GDPR, copyright, property theft, libel, fraud, discrimination and obscenity.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) are subject to the same requirements as technology provided by the school. All school devices used in and outside of school are monitored using Sophos & Schools Broadband DNA software to monitor for and inappropriate activity or activity that may place someone at risk.

The Computing Leader will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Practice for Pupils

Pupil access to the Internet is through a filtered service provided by Primary ICT, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

In addition, the following key measures have been adopted by Aberford C of E Primary School to ensure our pupils do not access any inappropriate material:

- Pupils using the Internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected programmes (see below).

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor Schools Broadband can accept liability under such circumstances.

The use of mobile phones by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff.

During school hours pupils are forbidden to play computer games unless specifically assigned by the teacher and should never access social networking sites.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline Policy. Minor incidents will be dealt with by the Computing Leader and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

Code of Practice for Staff

Staff have agreed to the following Code of Safe Practice:

- It is staff's responsibility to make themselves aware of GDPR regulations. The school has provided guidance that staff must follow in the Data Protection Policy.
- Pupils accessing the Internet should be supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed and are discussed with pupils.
- Any website used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate.
- Staff should only use their personal mobile phones during designated break times and never while there are pupils present. Personal mobile phones should not be visible except during staff break times.
- Staff accessing the internet within school should only ever use the school's internet system and should not be accessing any other online networks for any work related activity.

- Staff understand that any school device used is monitored through Sophos and Schools Broadband DNA software and any inappropriate activity will be logged with designated safeguarding leaders in school.
- Deliberate/ accidental access to inappropriate materials or any other breach of the school Code of Practice should be reported immediately to the Headteacher.
- In the interests of system security, staff passwords should only be shared with the Network Manager.
- Teachers are aware that Schools Broadband can track all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils must be taken with a school iPad (only when the headteacher has given specific permission can a camera be used to take photographs) which is password protected and images should be stored on a centralised area on the school network, accessible only to teaching staff. All images should not be held on personal cameras, phones or laptops.
- School systems may not be used for unauthorised commercial transactions.
- Staff should ensure that they do not allow parents or children to access their email address in the interest of personal safety (see below for what procedure to follow if this is breached).
- Children's names and images should not be shared on school twitter or any personal social media under any circumstances.

Protection of personal data

All staff must ensure they follow school policy and procedure to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Portable electronic devices, such as laptops that contain personal data are kept under lock and key when not in use. Documents and information are not saved to desktop areas on laptops but on the school server.
- All personal data is saved on the school network under individual staff folders or in secure shared files/drives. These are backed up by the school system and securely stored.
- Memory sticks and external portable hard drives are not to be used in school or to transfer or store any personal data.
- Passwords that are suitably secure and containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and ipads.

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. Staff accessing work emails on their personal mobile devices/tablets must ensure these are password protected.

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in the school's Data Protection Policy. Staff who have failed to follow policy and procedure may be personally liable in the event of a data breach.

Online Safety Awareness

At Aberford C of E Primary School we believe that, alongside having a written safety policy and Code of Practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for Pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed. In addition, all pupils follow a structured programme of Internet Safety Awareness using a range of online resources as part of the PSHE and Computing curriculum.

Internet Safety Awareness for Staff

The SLT keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is then disseminated to all teaching and support staff on a regular basis.

Health and Safety

Aberford C of E Primary School has attempted, as so far as possible, to ensure a safe working environment for pupils and teachers using Computing resources, which have been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards are being used.

Personal Safety

Parents and children should only have access the schools main email address or the email addresses set up to support children learning at home during COVID-19:

Office@aberfordceprimary.org.uk

Any emails that raise a potential pastoral or safeguarding concern or a parent query outside of curriculum or Teaching and Learning must be alerted to Mrs Crossley or a member of the SLT team immediately. The email should not be deleted, forwarded or copied until the member of staff has sought guidance from a member of SLT team.

Teachers and support staff should not allow either children or parents to use their school or personal email address. If a parent or child does access such information, the member of staff should print out any correspondence from the individual(s) and give a copy to Mrs Crossley Staff should not respond to any correspondence.

Digital and Video Images of Pupils

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school in the work in pupil's books, on notice boards and in school newsletters and brochures
- Outside of school by external agencies such as the school photographer, newspapers, publicity campaigns
- Online on our school website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

It is the responsibility of class teachers to check the consent that is in place for individual pupils prior to photographing/recording or displaying.

School Website

Our school website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Parental permission is acquired before any images are shared.
- Group photos are used where possible, with general labels/captions.
- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa.
- Only pupil's first names may be used. Full names should never be shared.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Storage of Images

Digital and video images of pupils are taken with school equipment such as a password protected iPad. Images are stored on a centralised area on the school network, accessible only to teaching staff.

Social Software

Chatrooms, blogs and other social networking sites are blocked by the School Broadband filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Online Safety Education for pupils. Instances of online bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's Discipline Policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.