CLIFTON ALL SAINTS ACADEMY

E-SAFETY/ACCEPTABLE USE POLICY

Revised : Spring 2018
Next revision : Spring 2021

Rationale

The requirement to ensure that pupils, staff and, indeed, all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound.

This framework of e-safety, or acceptable use policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other ‘child protection’ and ‘behaviour’ policies that the school already has in place as well as other existing policies in respect of its employees.

The intention of this evolving policy is:

- To maximise e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use

As such, the school more specifically intends:

1. To provide a secure network for the school and secure means of home/school access
2. To monitor traffic, log incidents and act accordingly
3. To establish key standards and behaviour for e-safety across the school, in-keeping with those of the Local Authority
4. To coordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents and governors
5. To ensure that we adhere to e-safety issues related to new government policies affecting schools
6. To monitor the school’s responses to e-safety matters and act accordingly
7. To have a named Senior Information Risk Officer (SIRO) to coordinate the development and implementation of e-safety policies, with clear designated responsibilities, and liaise with the Local Authority in such matters

E-safety is a whole-school issue and everyone in the school has a responsibility to promote it.

Guidelines

The policy aims to;

- To reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.

- enable young people to develop their own protection strategies when adult supervision and technological protection are not available;
- provide information on where to seek help and how to report incidents;
- help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online;
- provide guidelines for parents, carers and others on safe practice;
- ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders;
- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Strategy

All children will be able to make contributions towards the review of this policy through their work in ICT lessons. The policy will be put to the school staff and the Governors. Parents will be consulted via the website.

Passwords

Staff and pupil passwords are kept private and only the holder can change them. It is accepted that from time to time, e.g. forgetting a password, the ICT manager can help to create a new password but s/he will not know what it is. Computers must not be left in 'logged on' mode. (Ctrl + Alt + Delete, then Lock) It is good practice for users to change their password regularly, staff will change theirs every year in the Autumn term.

Emails

It is accepted that staff may send emails and attachments to recipients outside the school. Children may only do so under the supervision and direction of their teacher. During an ICT unit the staff member will e-mail the whole class on their individual learning platform account.

Pupils must immediately inform a member of staff if they received offensive e-mails.

Pupils must not reveal personal details/photos of themselves or others in e-mail communication

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system provided by Central Bedfordshire for DWM to use, which is updated regularly. The network is set up to automatically scan removable and other portable devices every time they are connected to the school system

Pod casting

Under the direct supervision of a teacher/LSA children may participate in pod casting to share with other schools.

Access to information

Information held by the school is defined and classified:

Restricted (named staff)	Protected (all in the school community)	Public (anyone)
Personal information related to pupils or staff (usually contained in the Management Information System)	School routines, schedules and management information	Website and promotional materials. Display material around school.
• Assessment Data e.g. SAT's results EYP data. • Photographs of the children kept in a central computer or staff laptops protected by a password. • Office computers • School e-mail system. • G & T and SEN lists. • Videos of the children within school	• ICT systems will be access via unique log-in and password. • Lists of children who participate in out of school events. • Curriculum planning.	• Learning Platform • Photographs on the wall around school. • School website. • Year 4 year book. • Event photographs e.g. sports/assembly

Access to all ICT systems shall be via a unique login and password. Any exceptions must be SIRO (Senior Information Risk Officer, the Head Teacher) approved. All information storage shall be restricted to necessary users with any additional access being SIRO approved. The SIRO must maintain a record of who has access to 'restricted' information.

Inappropriate content and language

The policy provides the following definitions of what is deemed 'inappropriate' for both email and website use.

Inappropriate email content: abusive, bullying, insulting, violent, threatening, sexual innuendo or offensive

> *e.g. material that can be construed as offensive on the grounds of gender, race, ethnicity, disability, sexuality, religion, age, size/stature, status, TU membership.

The type of language that is used in emails should be no different to that which is used in face to face situations.

Inappropriate web content: Children will be given a focus with which to search on the internet and will not be allowed free access at any time within school.

The SIRO will maintain an incident log and report on its use once a year to the governor responsible for ICT in their monitoring visit.

Staff

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies. Working at this school means acceptance of those policies, including this AUP.

As such:

- Staff must not allow any emails between themselves and pupils to be anything other than school business.
- Staff must not have any pupil (or former pupils) as 'on line' friends if they are of school age. Staff must report to the SIRO any contact from a pupil or former pupil of school age.
- During ICT lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials. In any instance of deliberate misuse the SIRO must be informed and the pupil will be dealt with in accordance with the school's behaviour policy.
- Staff need to be aware that conducting any personal transactions could result in residual information remaining on the hard drive which may be accessible to others**. Neither the school nor the Local Authority can accept any liability for any resulting loss or damage**.
- Staff will not use school laptops for personal shopping or social networking sites. Staff using social networking sites on personal computers will ensure that access to their pages is restricted.
- Staff should keep to a minimum any data which is held on their school laptop and they must lock it if it is left unattended (ctrl + alt + delete, lock).
- School laptops may be taken off site (with permission of the SIRO). Responsibility for their security lies with the staff member.
- PCs and laptops for pupils must be arranged in classrooms to allow good teacher supervision.
- Guidance to staff, in respect of the appropriate taking of images is provided in the school policy about photographs. It is not appropriate for staff members to use personal digital cameras or camera phones on field trips. Images should be transferred onto the school system under the direction of the ICT manager (refer to school policy about photographs)
- Parental permission will be sought for photographing children during school activities. Parents may restrict the use of the images to internal purposes only i.e. not for display or for the website.
- Photographs will be stored securely only on school devices.
- Any data that is taken away from the school premises must be securely encrypted on school devices and only accessed on those devices. Restricted data must be backed up by the Network Manager on a drive specifically set up for this purpose.
- Exporting data must only be on school devices.
- Mobile phones are not permitted in classrooms. Teachers and support staff must leave them in the staff room, helpers leave them in the office when signing in.

Pupils

Pupils will be taught about e-safety in KS1 and KS2 as part of the Computing curriculum.

- The school accepts the use of school email addresses by pupils to communicate with other pupils, to staff and to pupils in other schools providing they adhere to the pupil AUP.
- Pupils learn about the good practice that is appropriate for social networking during ICT
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.

If children accidentally find inappropriate material they are to report it to their teacher who will alert the SIRO so that s/he can take steps to rectify this. Staff who find inappropriate material will report it directly to the SIRO. Staff are made aware of their responsibilities in this during staff training and by having their own copy of the policy.

Sanctions

Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the SIRO. This policy will be reviewed every 3 years.

See new acceptable use policy for pupils attached.

Clifton All Saints Academy

ICT Acceptable use policy for Pupils

Pupils are involved, through the School Council and the work done in lessons in which activities to promote good practice and internet safety issues are delivered.

- Pupils are not to bring into school personally owned devices. If any such device is discovered an incident log must be completed and the device must be handed into the school office for safe keeping until such time as they can be collected by the parent/carer
- The school accepts the use of the VLE school e-mail addresses by pupils to communicate with other pupils and to staff providing they adhere to the pupil AUP(Acceptable use policy)
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.

As a responsible child at Clifton All Saints Academy;

- I will only log onto the VLE using my own user name and password.
- I will not reveal my password to others
- I will make sure all my ICT communication is sensible and responsible.
- I am responsible for my behaviour when using the Internet and VLE.
- I will not give out any personal information, such as my name, phone number, address or photograph.
- I will not give out any personal information about others.
- I will not browse for any material that is offensive or illegal.
- I will report any offensive or illegal material to my teacher.
- I understand that my teacher can read e-mails I send or receive.
- I will not copy material from the internet and say it is mine.
- I understand that if I do not follow this policy my parents/carers will be informed and a record will be kept.

Signed by .... (Name of Pupil)

Date................................

I have discussed this policy with my Child and will support the school's ICT Acceptable Use Policy;

Signed by;.. (Parent/Carer)

Date...