POPPY HILL
CHURCH OF ENGLAND MULTI ACADEMY TRUST

Acceptable Use Policy

Date to be reviewed	January 2027
Policy Status	Non Statutory
Responsible member	Karen Evans

This policy applies to all schools and stakeholders within Poppy Hill Academy Trust

Contents

Introduction

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.

Given the array of new technologies now available to use for educational purposes and in everyday life, 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:
- To provide a secure network for the school and secure means of home/school access
- To monitor traffic, log incidents and act accordingly
- To establish key standards and behaviour for e-safety across the school, in keeping with those of the Local Authority
- To co-ordinate 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
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the school's responses to e-safety matters and act accordingly
- To have a named Senior Information Risk Officer – (SIRO) – to co-ordinate 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, not something that is simply the responsibility of the ICT team and Operations Manager. As such, the whole school has a responsibility to promote it.

Guidelines

The AUP aims 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

This policy is the result of ideas discussed by the school community. The policy has been put to the school staff and ratified by the Governors. Parents are informed through the home/school agreement, guidelines distributed during Parents' Evenings and the pupils' AUP which is signed by them and their children at the beginning of the school year. E-Safety guidelines are displayed in the computer areas.

Hardware & Software

The school will provide staff with laptops where deemed necessary and on completion of a loan agreement form. This hardware is solely for the use of the member of staff to conduct school business. They are not to be used by any third party (i.e. family, friends etc). All hardware is maintained and repaired by our ICT support company Partnership Education in conjunction with the Operations Manager. Staff members are not permitted to attempt to fix suspected problems or allow any 3rd party to do so.

Staff members must not install any hardware or software without the permission of the Head Teacher or Operations Manager.

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 Operations 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. It is good practice for users to change their passwords regularly.

Emails

It is accepted that staff and Governors may send emails and attachments to recipients outside the school. Any data concerning pupils/parents or staff should be sent via the school email system ending in henlowacademy.org.uk as this is secure; such information should not be placed on memory sticks or sent via personal email. Children may only do so under the supervision and direction of their teacher.

The school reserves the right to check staff email accounts with prior notice to the member of staff the account belongs to, however, the school does not require permission to do this.

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system which is updated daily. The anti-virus software will automatically scan laptops and other portable devices every time they are connected to the school system.

Video Conferencing

Under the direct supervision of a teacher/TA children may participate in video-conferencing with other schools.

Restricted (Named Staff Only)	**Protected (All in School Community)**	**Public (Anyone)**
Any information that identifies an individual	Routines, management information	Website, parentmail, display

Access to all ICT systems shall be via logins and passwords. Any exception must be approved by the Operations Manager. All information storage shall be restricted to necessary users with any additional access being approved. The technician must maintain a record of who has access to restricted information

Inappropriate content and language

There will be zero tolerance to the use of inappropriate content and language on any ICT equipment within our school community. The school uses Impero to monitor content and language across devices.

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

Social Networking Sites

Staff and Governors must not include anything on their social networking sites (e.g. Facebook, Twitter), websites or email that relates to school in pictures or text and staff must not make any remarks relating to school business, children or staff without the permission of the Headteacher. Staff must be aware of their choice of language, content or of revealing personal details. Staff should also be aware that bringing the school into disrepute or breaching confidentiality will be a disciplinary matter. School hardware, including Chromebooks and laptops, should not be used to access personal social media of any description.

Children of school age or under should not be added to staff's social networking sites, nor should staff use e-mail etc. to communicate with them. This is for their own protection.

- Staff could be accused of grooming them.
- They could be exposed to inappropriate language etc from other "friends" on their site.
- Through their site they might access inappropriate material or people who might cause them harm.
- Children of that age are not supposed to be on "Facebook" so they are breaching the terms and conditions
- Parents may not be aware that children are using the site
- Their privacy settings may not be set securely.
- Any such connections should be blocked immediately. Infringements of this instruction may be regarded as a disciplinary matter.

Staff and Governors should not be discussing any matters regarding school, children, parents or other staff on Facebook or any other social networking site as these can also spread rapidly and bring the school into disrepute.

Photography, Videos and other Creative Arts

Many school activities involve the taking of images. These may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement.

Staff need to be aware of the potential for these aspects of teaching to be misused for pornographic or 'grooming' purposes. Careful consideration should be given as to how these activities are organised and undertaken. Particular regard needs to be given when they involve young or vulnerable pupils who may be unable to question why or how the activities are taking place.

Children who have been previously abused in this way may feel threatened by the use of photography, filming etc in the teaching environment.

The Governors have decided not to ban photography by parents at school events such as nativity plays or sports days. It is natural that parents would wish to have a record of their children at such happy points of their life.

Staff should remain sensitive to any children who appear uncomfortable and should recognise the potential for misinterpretation.

Using images of children for publicity purposes will require the age appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school have access. The school collects consent from parents/guardians and this should be checked prior to utilising photographs in this way.

It is recommended that when using a photograph the following guidance should be followed:

- if the photograph is used, avoid naming the pupil
- if the pupil is named, avoid using their photograph
- schools should establish whether the image will be retained for further use -

Images should be securely stored and used only by those authorized to do so by the headteacher. Phones, ipads or laptops which have photographs stored on them should be encrypted and/or password protected. Staff must not upload any school photos to social networking sites, regardless of the content, unless with the express permission of the Head Teacher.

Staff Visitors and Mobile Phones

Mobile phones should be switched off during work times unless required for work purposes (e.g. on school visits) or special permission is given by the SLT. If there is an emergency, staff can be contacted via the school office.

Personal phones should not be used to take photos or videos of pupils under any circumstances.

Personal calls should be kept to a minimum and made at appropriate times only. This includes texting.