This Policy was adopted by the governing body of

**Half Acres Primary Academy**

# E-SAFETY POLICY 2019

Dated: September 2019

Date for Review: September 2020

# 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# 2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

# 3. Roles and Responsibilities

## 3.1 The Local Governing Body

The local governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The local governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

## 3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT provider and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

### 3.4 The ICT Provider (Alamo)

The ICT Provider is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

### 3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

Help and support the school in supporting e-safety.
Read, understand and promote the school pupil AUP (Acceptable User Policy) with their children.
Take responsibility for learning about the benefits and the risks of using the internet and other technologies that their children use in school and at home.
Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
Model safe and responsible behaviours in their own use of technology.
Consult with the school if they have any concerns about their child's use of technology

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

### 3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

### 3.8 Pupils

Children in school will:

Read / understand and adhere to the pupil AUP (Acceptable User Policy).

Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates.

Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.

Take responsibility for their own and others' safe and responsible use of the technology in school and at home.

Respect the feelings, rights, values and property of others in their use of technology in school and at home.

Understand what action they should take if they are worried, uncomfortable, feel vulnerable or at risk whilst using technology in school and at home, or if they know of someone this is happening to.

• Discuss e-safety issues with trusted adults in an open and honest way.

# 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and focus weeks to raise pupils' awareness of the dangers that can be encountered online and may invite speakers to talk to pupils about this.

# 5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, Inspire workshops and in information via our website

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and then the Headteacher/ DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

# 6. Cyber-bullying

## 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

## 6.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff find regular opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also makes information/leaflets on cyber-bullying available to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. The Headteacher/DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the Headteacher/DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. Acceptable Use Of the Internet In School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Each time they log on to a school machine they will agree to the terms of the agreement. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

**A general guide to the use of technology in our school:**

| Device | Children | Staff |
|---|---|---|
| Mobile phones | Not allowed – if any phones are brought to school by children, they should be kept in the school office until the end of the school day | Staff allowed in own time (see also Professional Standards Policy) |
| *I Watch (devices linked to phones)* | Not allowed | *Staff to modify use in line with other mobile technologies eg alerts to be turned off during working hours* |
| Taking photos or videos on school equipment | Allowed if supervised by an adult | Staff allowed - must adhere to the 'Safe use of Images'. Staff taking photos or videos must move to their laptop and delete from the ipad. |
| Taking photos or videos on personal equipment | Not allowed –exceptions made for residential visits when staff outline rules for use | In exceptional circumstances, staff allowed - must adhere to the 'Safe use of Images' |
| Use of handheld devices eg MP3 players, personal gaming consoles | Not allowed | Staff allowed in own time |
| Use of personal email addresses in school | Not allowed | Staff allowed on school owned laptops in own time |
| Use of school email addresses for personal correspondence | Not allowed | Not allowed except in circumstances agreed with the Headteacher |
| Use of on-line chat rooms | Not allowed | Not allowed |
| Use of instant messaging services | Not allowed | Staff allowed on school owned laptops in own time |
| Use of blogs, wikis, podcasts or social networking sites | Not allowed unless specifically set up by a member of staff for educational purposes | Not allowed – except if set up in connection with their work and with SLT permission |
| Use of video conferencing or other on line video meetings | Not allowed – except if set up and supervised by staff for educational purposes | Not allowed – except if set up in connection with their work and with SLT permission |

**E-MAIL and other forms of electronic communication**

Much of our communication in school is managed via email. All staff have an email account linked to the school system and this email address should be the one used for all school-linked correspondence. Any information about a child(ren) sent to anyone via email must be secure through the use of codes, passwords and avoiding using the full name of a child. These expectations on the sharing of information are equally valid if the communication is via Twitter or any other form of electronic communication.

Pupils will be reminded when using electronic communication about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening messages from an unknown sender and opening/viewing attachments. Children cannot access personal email accounts during school.

Email encryption should always be used for communicating sensitive information.

Mobile Device Management must be used for staff accessing school email through their mobile devices to ensure the protection of data in line with GDPR.

Communication between staff and pupils and members of the wider school community should be professional and related to school matters only. Staff must not be in communication with any

parents or children via Facebook or any similar social media. If any parents or children approach any staff to 'befriend' them using such media the staff member must inform a senior leader. Any inappropriate use of school technology for communication or the receipt of any inappropriate messages by a user, should be reported to a senior leader immediately.

**Use of Mobile Phones**

Where staff are required to use a mobile phone for school duties, for instance in case of emergency during off site activities, and the school mobile phone is not available, they should contact the school, who will contact the parent or relevant personnel/authorities. Staff should not use their own personal phone giving parents access to their personal contact details.

**The School Website and Twitter**

All content on the school website will be approved by the Headteacher before publication
Only parents who complete a school form will be permitted to follow the school's Twitter feed.
A generic contact e-mail address will be used for all enquiries received through the school website.
The school website will not include any personal details, including individual e-mail addresses, or full names of staff or pupils.

## 8. Pupils Using Mobile Devices in School

Pupils who bring mobile phones to school should leave them in a secure designated place (school office) for the duration of the school day. The school is not responsible for any lost, misplaced or stolen phones.

## 9. Staff Using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT provider.

## 10. How the School Will Respond to Issues of Misuse

To support parents we will regularly share information outlining how they can support their children to be safe, what to be vigilant for and organisations they can contact for further support and advice.
If we ever have to deal with an e-safety incident in school, or if an issue is brought to our attention, we will always contact parents so they are informed and can take any relevant action at home if this was necessary.
All users must report any incidents of accidental access to inappropriate materials immediately to a senior leader.

Deliberate access to inappropriate materials by any user will lead to the incident being logged and dealt with as a serious incident. This will be investigated fully by a senior leader. There will almost certainly be serious consequences of any such behaviour.

For a child we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.This could, in extreme circumstances, result in an exclusion.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. This could result in suspension, possibly leading to dismissal and involvement of the police for very serious offences. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**COMPLAINTS**

Complaints relating to e-safety should be made to the Headteacher. Incidents should be logged.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with the academy's child protection procedures.
Parents will be informed of the complaints procedure (see the MAT complaint's policy).

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

## 12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in the appendices.

This policy will be reviewed at least annually by the Headteacher in consultation with the ICT provider. At every review, the policy will be shared with the governing board.

## 13. Links with Other Policies

This online safety policy is linked to our:

Safeguarding Policy

Behaviour Policy

Staff Disciplinary Procedures

Data Protection Policy and privacy notices

Complaints Procedure

| | | | |
|---|---|---|---|
| Signed by Acting Headteacher |  | Date: | 03.10.2019 |
| Signed by Chair of Governors |  | Date: | 03.10.2019 |

**Staff and Other Adults in School – Acceptable Use Agreement**

**Technology such as computers, laptops, ipads, email, the internet and mobile phones are an expected part of our daily working life in school. This agreement is to help ensure that all staff are aware of their professional responsibilities when using any form of technology and to help keep staff, governors and visitors safe. All staff are expected to follow this agreement and adhere to its contents at all times. Any concerns or clarification should be discussed with the Headteacher.**

• I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
• I will comply with the technology system security and not disclose any passwords provided to me by the school or other related authorities.
• I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
• I will not give out my own personal details, such as mobile phone number or personal email address, to pupils or parents.
• I will only use the approved email system for any communications with pupils, parents and other school related activities.
• I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body and with appropriate levels of security in place.
• I will not install any hardware or software on school equipment without the permission of the Headteacher.
• I will report any accidental access to inappropriate materials immediately to a senior leader.
• I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
• Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or head of school in line with data security policy.
• I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Headteacher.
• I will respect copyright and intellectual property rights.
• I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
• I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of technology.

**User Signature**

I agree to follow this acceptable use policy and to support the safe use of technology throughout the school

Signature …… Date ……Full Name ……(printed)

**Half Acres Academy**
**Pupil Acceptable Use Agreement**

• I will only use technology in school for school purposes.
• I will only use my own school email address (if appropriate) when emailing.
• I will only open email attachments from people I know, or who my teacher has approved.
• I will not tell other people any of my passwords relating to school sites eg Times Tables Rockstars.
• I will only open/delete my own files.
• I will make sure that all technology related contact with other children and adults is appropriate and polite.
• I will not deliberately look for, save or send anything that could offend others.
• If I accidentally find anything inappropriate on the Internet, I will tell my teacher immediately.
• I will not give out my personal details such as my name, phone number, home address or school.
• I will be responsible for my behaviour when using technology in school or at home because I know that these rules are to keep me safe.
• I will not arrange to meet someone.
• I know that my use of technology can be checked and that my parent or carer contacted if a member of school staff is concerned about my safety.

Name of Child…….  Signature Pupil……

Signature Parent……

Appendix 3

| **E- Safety Incident/Concern Form**<br><br>Please complete as soon as possible and return to the designated person<br><br>School name…… Designated Senior Leader……. |
|---|

| | |
|---|---|
| Name: | |
| Date /time/ place (home or school) of concern: | |
| Nature of concern/Incident | |
| Evidence eg text, email.Is the evidence still available? | |
| Reported by:<br><br>Designation | |
| Other witnesses: | |
| Reported to: | |
| Signed: | Witness |
| Signed: | Designated Senior Person |
| Action (completed by designated leader) | |
| Outcome: | |