| | |
|---|---|
| Produced By: | Ass. HT |
| Last amended | May 2020 |
| Approved by Management Com. | n/a |
| Date for Review: | May 2022 |

## The Key Education Centre

**Online Safety Policy**

**Contents**

*Remit*
*Context*
*Roles and Responsibilities*
*Managing Internet Access and Network Safety*
*Managing Published Content*

*Appendices:*

1. *Parent E-safety Agreement Form*
2. *KS1 Pupil E-safety Agreement Form*
3. *KS2 Pupil E-safety Agreement Form*
4. *12 Rules for Responsible ICT Use*
5. *Staff Acceptable Use form.*

**Remit:**

Our E-Safety Policy has been written by the school, based on Government guidance and best practice. It has been agreed by the Leadership Team. The E-Safety Policy will be reviewed annually.

This policy applies to all members of the school community (including staff, students / pupils, management committee, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

This Policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Mobile Phone Policy

**Context:**

The use of the Internet in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, all schools are duty bound to ensure that children and young people are able to use these exciting and innovative technologies appropriately and safely; the use of these new technologies can put young people at risk within and outside the school. Some of the dangers our pupils may face include:

**Content:**

- Exposure to illegal, harmful or inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation (how to check authenticity and accuracy of online content)

**Contact:**

- Unauthorised access to / loss of / sharing of personal information, including personal images
- Grooming (sexual exploitation, radicalisation etc)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Inappropriate communication / contact with others, including strangers
- Access to unsuitable video / Internet games

**Conduct:**

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting (see guidelines in Safeguarding Policy).
- Copyright (little care or consideration for intellectual property and ownership)

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, mobile phone and safeguarding and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to, and families' awareness of, the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

**Roles and Responsibilities:**

**Headteacher / Senior Leaders:**

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety will be delegated to the Assistant Headteachers and Designated Safeguarding Leads.

The Headteacher is responsible for establishing and reviewing the school e-safety policies / documents and the implementation and effectiveness of this policy.

The Headteacher / Senior Leaders are responsible for ensuring that all staff receive suitable CPD to enable them to carry out their e-safety roles.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support for those colleagues who take on monitoring roles.

The Headteacher and Assistant Headteachers should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff and liaise with the Local Authority as appropriate. (See Managing Allegations against a member of staff policy/guidance)

**Assistant Heads:**
Assistant Heads take day to day responsibility for e-safety issues and ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Assistant Heads report to the Headteacher serious breaches of the E-Safety Policies, provide training and advice for staff, receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.

**Teaching and Support Staff:**
Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the E–Safety policy, school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Designated Safeguarding Lead for investigation / action / sanction
- digital communications with pupils and parents / carers (email / voice) are on a professional level
- students / pupils understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy
- students / pupils understand and follow E-Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with behaviour and anti-bullying policies
- in lessons where internet use is planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

**Designated Safeguarding Leads:**
Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting (guidelines in Safeguarding Policy)
- revenge pornography

- radicalisation (extreme views)
- CSE

**Pupils:**
- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability
- will be expected to follow school rules relating to this policy eg safe use of cameras, IPads, cyber-bullying etc
- should understand that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

**Parents / Carers:**
Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers often do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy
- reading, understanding and promoting the school's Pupil Acceptable Use Agreement with their child(ren)
- consulting with the school if they have any concerns about their children's use of technology
- supporting the school in promoting online safety and endorsing the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

**Managing Internet Access and Network Safety:**

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirements for Hampshire Local Authority
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- The school maintains and supports the managed filtering service provided by Hampshire Local Authority through flexible web filtering.
- Remote management tools are used by Hampshire Local Authority to control workstations and view users' activity
- Appropriate security measures are in place, provided by Hampshire Local Authority, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- Guest access to the school network will be limited to guest wifi which does not give access to personal information about pupils or staff
- The school infrastructure and individual workstations are protected by up to date anti-virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy.

**Managing filtering:**
- The school has filtered Internet access through the Hampshire Network
- If staff or pupils discover an unsuitable site, it must be reported to the service provider (Hants) so that unsuitable sites can be blocked.

**Social networking and personal publishing:**
- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils and that age limits apply to older pupils.

**Staff access and acceptable use:**
All staff are required to read and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the work place. This will be signed when they commence their employment at The Key and will be reinforced each year during the staff's E-Safety Session. All staff will attend both training on E-Safety and Prevent (dealing with radicalisation and extremism).

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: ie E-mail, Internet, Intranet and network resources, software, equipment and systems and complements the General Teaching Council's Code of Practice for Registered Teachers.

**Managing Published Content:**

**School web site:**
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility for the main site and ensure that content is accurate and appropriate. SLT will take responsibility for their own site information and ensure that content is accurate and appropriate.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website; permission will also be sought informally from children themselves.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' names will not be used anywhere on the school web site or, particularly in association with photographs.

**Mobile Phones and Devices:**

- Mobile phones should not be used during lessons or formal school time, in classrooms, corridors or in outside areas. If staff need to use a mobile phone in case of emergency, they should go to the main school office or staff room.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer. Staff will be issued with a school phone where contact with pupils is required.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff must ensure that there is no inappropriate or illegal content on any device brought into school or held in school.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

**E-Mail:**

When using communication technologies the school considers the following as good practice:

- The school will communicate with the staff via Outlook staff email
- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to SLT the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and other stakeholders, eg external organisations, students or parents / carers must be professional in tone and content and be via official used systems, not personal email accounts.
- The forwarding of chain letters is not permitted.
- Teachers are expected to monitor the use of Pupil Mail when used.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.

**Responding to Incidents of Misuse:**

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. The incident should be dealt with in accordance with the safeguarding policy and, if necessary, the police should be informed if any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity ie:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with by the Designated Safeguarding Lead as soon as possible in a proportionate and appropriate manner.

# Appendix 1: E-safety agreement form: parents

**Parent / guardian name: …….**

Pupil name: ……..

As the parent or legal guardian of the above pupil, I grant permission for my daughter or son to have access to use the Internet, e-mail and other ICT facilities at school.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the 12 ‘rules for responsible ICT use’.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child’s computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

Parent / guardian signature: ……

Date: ……

# Appendix 2: E-Safety Agreement Form: KS2

## Keeping safe: stop, think, before you click!

Pupil name: _____

- ✓ I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.
- ✓ I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.
- ✓ This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.
- ✓ I understand that the school can check my computer files, and the Internet sites I visit and that if they have concerns about my safety, that they may contact my parent / carer.

Pupil's signature: ……..

Date:
…….

## Appendix 3: E-Safety Agreement Form KS1

# *Think before you click*

S

**I will only use the Internet and email with an adult**

A

**I will only click on icons and links when I know they are safe**

F

**I will only send friendly and polite messages**

E

***If I see something I don't like on a screen, I will always tell an adult***

My Name:

My Signature:

**Appendix 4: 12 rules for responsible ICT use**

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers when given permission by an adult.
- I will not look at or delete other people's files without permission.
- I will keep my login and password secret.
- I will not bring files or CDs/USBs into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit or try to access Internet sites I know to be banned by the school and I will use the Internet responsibly.
- I will only e-mail people I know or my teacher has approved and the messages I send will always be polite and sensible.
- I will not open an attachment or download a file unless I have permission.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever met on the Internet or by email or in a chat room, unless my parent or guardian has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a responsible adult.

Appendix 5: Staff Acceptable Use Policy

## Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head of School.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.

- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school’s e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

## Acceptable Use Policy (AUP): Staff agreement form

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school’s ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

**Authorised Signature (Head of School)**

I approve this user to be set-up.

Signature ..... Date.....

Full Name ..... (printed)