Hoyland Common Academy Trust
E-Safety Policy
2017

HOYLAND COMMON ACADEMY TRUST E SAFETY POLICY

Please note:

This policy has been developed between key advisors, the trade unions represented at the school and professional associations recognised by Hoyland Common Academy Trust who have been consulted in the development of this policy.

Introduction

Hoyland Common Academy Trust is committed to safeguarding all members of the school community. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Hoyland Common Academy Trust educates children, parents and staff about the benefits, risks and responsibilities of using information technology.

How will Internet use enhance learning?

Developing good practice in Internet use as a tool for teaching and learning is clearly essential. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Often the quantity of information needs to be cut down and staff guide pupils to appropriate Web sites, providing them with specific questions to answer, by publishing lists on the school website and to parents through newsletters and parent meetings and by including them in year group Favourites. Internet access will be planned to enrich and extend learning activities. Pupils will be taught what Internet use is acceptable, how to use the internet safely and given clear objectives for Internet use in line with the AUP. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The role of the Head of School:

The Head of School has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety Co-ordinator. The Head of School (Designated Safeguarding Lead) and Deputy Safeguarding Lead are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. The Head of School is responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Head of School 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. The Head of School will receive regular monitoring updates from the E-Safety Co-ordinator.

The role of the E-Safety Coordinator:

The e-safety coordinator takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. They ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and provide training

and advice for staff. When e-safety incidents are reported the e-safety coordinator creates a log to inform future e-safety developments.

The role of the IT support team:

The IT support team (EAST) is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack. Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. They are responsible for ensuring that internet filtering is applied and updated on a regular basis and that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School for investigation.

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. That they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP). Staff must report any suspected misuse or problem to the Head of School/E-Safety Coordinator for investigation, action or sanction. All staff should ensure that e-safety issues are embedded in all aspects of the curriculum and other activities and that e-safety practises are modelled to children. Staff must ensure that pupils understand and follow the e-safety and acceptable use policies and that they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices. In lessons where internet use is planned, 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.

Pupils:

Pupils are educated in e-safety practises and responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Pupils will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying. They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

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. The school will take every opportunity to help parents understand these issues through parent's evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

E-Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of

the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable

Safeguarding our children on the Internet

While the internet provides access to a world of new information and points of view, it also exposes young people to very real harms. Often children are left to access the internet without any supervision or controls and it can lead to danger from grooming, inadvertent exposure to graphic images, radicalisation and other online threats. So much time is now spent online that keeping children safe as well as enabling them to 'stay children' is paramount. The Safeguarding Policy for HCAT makes reference to such threats.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

http://www.proceduresonline.com/barnsley/scb/p_esafety_abuse_dig_media.html?zoom_highlight=internet

Technical – infrastructure / equipment, filtering and monitoring

With guidance from the IT support team (EAST) 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. There will be regular reviews and audits of the safety and security of technical systems. Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school technical systems and devices.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless express parental permission has been sought beforehand. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of an agreement signed by parents or carers at the start of the year)

Communication

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Mobile technologies

Mobile phones are not permitted to be used in the EYFS setting. Staff are permitted to use their mobile phones in the office and in the staff room area, but the taking of photographs on mobile phones is strictly prohibited anywhere within the EYFS setting.

Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Staff Acceptable Use Policy Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites**.**
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones).

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and the e-Safety Coordinator. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Team (EAST) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: …… Print Name: …… Date: ……

Accepted by: …… Print Name: ……

Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Policy (AUP).

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name of Pupil
Group / Class
Signed Date

Acceptable Use Policy for Young Children

This is how we stay safe when we use computers:

I will ask a teacher / an adult if I want to use the computer.
I will only use activities that the teacher /an adult has told or allowed me to use.
I will take care of the computer and other equipment.
I will ask for help from the teacher / an adult if I am not sure what to do or if I think I have done something wrong.
I will tell the teacher / an adult if I see something that upsets me on the screen.
I know that if I break the rules I might not be allowed to use a computer.

Signed (child):.....

Signed (parent): .....

Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's e-safety.

Signed

Date