Ocker Hill Academy
e-Safety Policy
Contents

Our e-Safety Policy has been written by the academy, building on the Becta guidance.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging (IM)
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Ocker Hill Academy, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the academy (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto academy premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the academy, the Principal and governors have ultimate responsibility to ensure that the policy and

practices are embedded and monitored. The named e-Safety co-ordinator in our academy is Mr Hollyhead (Principal) who has been designated this role as a member of the senior leadership team. All members of the academy community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Sandwell LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal/ e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our academy in relation to local and national guidelines and advice.

This policy, supported by the academy's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole academy community. It is linked to the following mandatory academy policies: child protection, health and safety, home–academy agreement, and Social Inclusion (including the anti-bullying) policy and PHSE.

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of INSET.
- Details of the ongoing staff training programme can be found in the CPD File, CPD Policy and Teaching and Learning Guidelines.
- New staff receive information on the academy's acceptable use policy, and Mobile IT Policy, as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the academy community.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the academy e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each academy year.
- e-safety posters will be prominently displayed in appropriate areas.

e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The academy has a framework for teaching internet skills in ICT lessons.
- The academy provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside academy is done informally when opportunities arise and as part of the PSHE curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ Learning Mentor, and/ or an organisation such as Childline.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

Password Security (Ref- Data Protection Policy)

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords **which are not shared with anyone.** The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the academy's e-safety Policy.
- Users are provided with an individual email and Learning Platform log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the academy network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to a member of the SMT.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of academy networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

- In our academy, all ICT password policies are the responsibility of the Principal and all staff and pupils are expected to comply with the policies at all times.

Data Security (ref – Data Protection Policy)

The accessing and appropriate use of academy data is something that the academy takes very seriously. The academy follows Becta guidelines (published Autumn 2008)

- Staff are aware of their responsibility when accessing academy data e.g. academy SIMS Systems, FMS and admin server. The level of access is determined by the Principal
- The academy do NOT authorise for any data to be taken off the academy premises unless encrypted (in special circumstances – here staff should seek advice from the Academy Technician)
- Data can only be accessed and used on academy computers or laptops (via the remote Gateway) Staff are aware they must not use their personal devices for accessing any academy/ children/ pupil data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of Sandwell Broadband is logged and the logs are randomly but regularly monitored. **Whenever any inappropriate use is detected it will be followed up. In the event of any suspicious activity or inappropriate web site access/ pop ups – these must always be reported to the Principal immediately.**

- The academy maintains pupils will have supervised access to Internet resources (where reasonable) through the academy's fixed and mobile internet technology.
- **Staff will preview any recommended sites before use.**
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- The Local Authority has a monitoring solution via Sandwell Broadband where web-based activity is monitored and recorded.
- Academy internet access is controlled through the LA's web filtering service.
- Ocker Hill Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that academy based email and internet activity can be monitored and explored further if required.
- The academy does not allow pupils access to internet logs.
- The academy uses management control tools for controlling and monitoring workstations.
- **If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator (Technologies Coordinator/ Principal)**
- It is the responsibility of the academy, by delegation to the Technician, to ensure that Anti-virus protection is installed and kept up-to-date on all academy machines.
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the academy's responsibility nor the Technician's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the **technician** for a safety check first.
- Pupils and staff are not permitted to download programs or files on academy based technologies without seeking prior permission from **the Principal.**
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Gateway.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. **To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.**

- **At present, the academy endeavours to deny access to social networking sites to pupils within academy.**
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the

appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, academy details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the academy.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Principal.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and smart phones are familiar to children outside of the academy too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in the academy is allowed. Our academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately;

1. **Personal Mobile devices (including phones)**

- The academy allows staff to bring in personal mobile phones and devices for their own use, but must keep them switched off during academy time (unless otherwise agreed with the Principal). **Under no circumstances does the academy allow a member of staff to contact a pupil or parent/carer using their personal device.**
- Pupils are not allowed to bring personal mobile devices/phones to the academy. For confiscation of such items – ref Social Inclusion Policy.
- **The academy is not responsible for the loss, damage or theft of any personal mobile device.**
- The sending of inappropriate text messages between any members of the academy community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the academy community.
- Users bringing personal devices into academy must ensure there is no inappropriate or illegal content on the device.

2. Academy provided Mobile devices (including phones)

- Permission must be sought before any image or sound recordings are made on the devices of any member of the academy community.
- Where the academy provides mobile technologies such as phones and laptops for offsite visits and trips, only these devices should be used.
- Where the academy provides a laptop for staff, **only this device may be used to conduct academy business outside of the academy.**

Managing email

The use of email within most academies is an essential means of communication for both staff and pupils. In the context of the academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between academies on different projects, be they staff based or pupil based, within the academy or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The academy gives all staff their own email account to use for all academy business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all academy business.
- Under no circumstances should staff contact pupils, parents or conduct any academy business using personal email addresses.
- The academy requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the academy'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on academy headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Principal, line manager or designated account.
- Pupils may only use academy approved accounts on the academy system and only under direct teacher supervision for educational purposes.
- Pupils have their own individual academy issued email accounts via the Gateway (from 09/10)
- The forwarding of chain letters is not permitted in academy.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

- Staff must inform the Principal if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore can be misused. We must remember that it is not always appropriate to take or store images of any member of the academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and verbal consent of staff, the academy permits the appropriate taking of images by staff and pupils with academy equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips – unless the written photo permission has been sought. **However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the staff device once completed.**
- **Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.**

Consent of adults who work at the academy

- Permission to use images of all staff who work at the academy is sought on induction training/ policy familiarisation and any staff objecting to this MUST inform the Principal immediately.

Publishing pupil's images and work

On a child's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the academy's web site
- on the academy's Learning Platform
- in the academy prospectus and/or other printed publications that the academy may produce for promotional purposes (education related only)
- recorded/ transmitted on a video or webcam
- in display material that may be used in the academy's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the academy
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire year and is reviewed annually. If there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc then a new permission may be sought during the academic year.
Parents/ carers may withdraw permission, in writing, at any time.

Consent has to be given by parents/carers in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Technician has authority to upload to our website.

Storage of Images

- Images/films of children are stored on the academy's network (MIS) / Gateway (ONLY)
- **Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Principal**
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the academy network/ Learning Platform.
- The administrative team/technician has the responsibility of deleting the images when they are no longer required, or the pupil has left the academy.

Webcams and CCTV

- The academy uses CCTV for security and safety. The only people with access to this are the Senior Management Team and Chair of Governors. Notification of CCTV use is displayed around the academy.
- We do not use publicly accessible webcams in the academy.
- Webcams in the academy are only ever used for specific learning purposes, i.e. links with other academies.
- Misuse of the webcam by any member of the academy community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Webcams can be found in the ICT Suite. Notification is given in this/these area(s) filmed by webcams by signage when in use (this is the responsibility of the staff user)
- Consent is sought from parents/carers and staff on joining the academy, in the same way as for all images.

Video Conferencing

- Permission must be sought from parents and carers if their children are involved in video conferences.
- All pupils must be supervised by a member of staff when video conferencing.
- All pupils must be supervised by a member of staff when video conferencing with end-points beyond the academy.
- The academy will keep a record of video conferences, including date, time and participants.
- Approval from the Principal must be sought prior to all video conferences within the academy.
- The academy conferencing equipment, if used, should not be set to auto-answer and is only to be switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Staff MUST consider and discuss with the SMT before engaging in conferencing:

- If participants in conferences offered by 3rd party organisations then we DO insist on enhanced CRB disclosure numbers, dates of issue etc.
- Conference supervisors (staff) need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the Principal. Incidents should be logged (see appendix)

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct through staff training, parent consultation and pupil/parent e-safety annual agreements.

Equal Opportunities

Pupils with additional needs

The academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the academy's e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of the academy. We consult and discuss e-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the academy e-Safety policy through an annual review.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the academy / on an annual basis.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain.
- The academy disseminates information to parents relating to e-Safety where appropriate in the form of;
    - Posters (in the academy)
    - Website/ Learning Platform postings (where appropriate)
    - Newsletter items
    - Parent meetings
    - Letters

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

Staff and pupils have been involved in making/reviewing the e-Safety policy through staff meetings and academy council meetings.

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them. This policy will be reviewed every 12 months and consideration given to the implications for future whole academy

development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, Principal and governors in November 2013.