Shireland Hall Primary Academy

Online Safety Policy

Reviewed by Claire Quinn September 2018
Next review September 2019

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 equip our young people with the skills to access lifelong 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
- Instant Messaging apps (eg WhatsApp, Kik)
- Photo and video sharing apps (eg Instagram, Snapchat)
- Chat Rooms, Forums and Social Networks (eg Twitter, Facebook)
- Youtube Channels
- Blogging and Vlogging
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Online Gaming including instant chat
- Mobile / Smart phones with functionality including text, camera, video, web-browsing, audio, music , GPS
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

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

Ensuring that children and young people are aware of the risks associated with the use of technologies, and can adopt safer online behaviours, is vital in safeguarding them against cyberbullying, grooming and radicalisation.

At Shireland Hall Primary Academy we understand the responsibility to educate our pupils on Online 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,both inside and outside of the classroom.

This policy relates to both fixed and mobile internet technologies provided by the academy, as well as those technologies owned by pupils, parents and staff, but brought onto academy premises.

Roles and Responsibilities

The Executive Principal and governors have ultimate responsibility to ensure that this policy and its practices become embedded and are monitored. The named Online Safety Coordinator in our academy is Claire Quinn, Assistant Principal and Designated Safeguarding Lead, 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 coordinator to keep abreast of current issues and guidance.

Senior Leaders and Governors are updated by the Executive Principal/ Coordinator 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, 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 agreements, and behaviour/pupil discipline (including the anti-bullying) policy and particularly to the curriculum for PHSE, Learning for Life and Computing.

Skills/awareness development for staff

- Our staff receive regular information and training on Online Safety issues in the form of staff meetings.
- New staff receive information on the academy's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of and know what to do in the event of misuse of technology by any member of the academy community.
- All staff are expected to incorporate activities and awareness within their half-termly discrete Online Safety lessons as well as each time they use computers, laptops and iPads within any area of the curriculum.

Managing the academy Online Safety messages

- We endeavour to embed messages across the curriculum whenever the internet and/or related technologies are used. This is particularly reinforced in Computing lessons and PSHE lessons in relation to cyberbullying, grooming and radicalisation.
- The policy is be introduced to the pupils at the start of each academic year.
- Online Safety posters are prominently displayed in each classroom and on all laptop and iPad trolleys.
- The academy uses RM Community Connect 4 software. This system reminds users of their obligations as a condition of logging in.
- A display board with key Online Safety messages is displayed downstairs in a corridor easily accessible by all pupils.
- Half-termly assemblies led by the Computing Leader and pupil Digital Leaders also communicate Online Safety Messages

ICT in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for guidance to be given to the pupils on a regular and meaningful basis.

- Educating pupils on the dangers of technologies that may be encountered outside academy is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about the dangers of sharing personal information online through discussion, modelling and activities.
- Pupils are taught about copyright and respecting other people's information and intellectual property 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/older sibling, teacher/trusted staff member, or an organisation such as Childline or the CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher modelling, discussions and via the Computing curriculum.
- Half-termly Computing and Learning for Life lessons provide the opportunity to discuss issues relating to cyberbullying, sexting, grooming and radicalisation (eg: through respect for others and appropriate/positive relationships) These

lessons can equip pupils with the knowledge to keep safe from harm.

Password Security

Password security is essential for staff, particularly as they are able to access and use personal pupil data. Staff are expected to have secure passwords which are not shared with anyone.This is also in line with General Data Protection Regulations 2016. All staff receive regular training and briefing reminders about this. The pupils are expected to keep their passwords secret and not to share with others, not even with their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read ***and sign*** an Acceptable Use Policy to demonstrate that they have understood and agree to the academy policy.
- Pupils are provided with an individual network log in username. From Year 2 they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access online materials or files on the academy network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to the Network Manager (Peter Mason).
- Staff are aware of their individual responsibilities to protect the security and confidentiality of academy networks, MIS systems and Learning Platform, including ensuring that passwords are "strong" and not shared. Staff do not save passwords when using programs such as google chrome.Individual staff users must also make sure that workstations are locked when they are away from their computer.
- Staff do not share their logged on workstation with another member of staff.

Data Security

The accessing and appropriate use of academy data is something that the academy takes very seriously.

- The academy network is backed up daily onto digital media stored in the academy's safe.

Staff will:

- Only use data off the academy premises via an encrypted website e.g. ScholarPack, informing SLT before they do so.
- Not allow family members or friends to use the computer while logged in remotely to academy resources.
- Never share passwords/leave on post-it notes etc.

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. In our academy internet use is logged using Impero software and the logs are randomly but regularly monitored by the Network Manager. Whenever any inappropriate use is detected it is followed up immediately

- In our academy pupils are not allowed unsupervised access to the Internet.
- Staff will preview any recommended sites before use with pupils.

Infrastructure

- Academy Internet access is controlled through RM SafetyNet
- Shireland Hall Primary Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998,The General Data Protection Regulations 2016. 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 or blogs.The academy uses Impero management control tool 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 co-ordinator.
- Anti-Virus protection is provided by Trend Micro and is set to automatically update on all academy machines. This is the responsibility of Peter Mason, network manager.
- Privacy Impact Assessment are in place for monitoring

software/new software that is being introduced to Academy staff, pupils and parents.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. 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 denies access to social networking sites to pupils and staff 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, email addresses/usernames, specific hobbies/interests).
- Pupils are asked to report any incidents of cyberbullying to the academy immediately
- Staff understand that it is not acceptable to use social networking sites and other personal communication tools to communicate with pupils and/or parents (eg Facebook, Twitter, email etc).
- Staff understand that it is considered a disciplinary offence if they mention on social networking sites issues concerning pupils/parents/carers/other staff associated with the academy.

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 smart phones, tablets and gaming devices) are familiar to children outside of the academy. Allowing

such personal devices to access the academy network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc.
Emerging technologies are examined for educational benefit and the risk assessed through Privacy Impact Assessments before such use of personal devices is facilitated in the academy. Our academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The academy allows staff to bring in personal mobile phones and devices for their own use in line with Academy Mobile Phone Policy. Under no circumstances does the academy allow a member of staff to contact a pupil or parent/carer using their personal device.
- Staff may not record or take photos of any child using their personal device.
- EYFS is a "No" phone zone.

- Pupils in YR5/6 are allowed to bring personal mobile phones to academy for contact with family when walking to/from school daily but must not use them for personal purposes within lesson time and these are kept in the SLT office.
- Technology Is used for educational purposes, as mutually agreed with the Executive Principal/teacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the academy community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on these devices of any member of the academy community. If these are intended to be published on school website or on school social media accounts, consent is sought before any image/video/sound is published. Consent is recorded on Scholarpack with the local Compliance Officer.
- Capturing images & video is not allowed by pupils/staff unless on academy equipment and for educational purposes.
- Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

Academy-provided Mobile devices (including phones)

- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the academy community.
- Where the academy provides mobile technologies (eg phones, laptops) for off site visits and trips, only these devices are used.

Managing email

The use of email within most academies is an essential means of communication for staff, parents and sometimes pupils. In the context of the academy, email is not be considered private. Educationally, email can offer significant benefits including; direct written contact between academies on different projects, be they staff- or pupil-based, within the academy or internationally. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good online etiquette. In order to achieve the expected standard for Computing, pupils must have experienced sending and receiving emails.

- The academy gives all staff a business email account to use for all academy purposes. . This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed.
- Staff including Governors should never use their personal email account(s) for any academy purposes..
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff email addresses are be used for all academy business.
- Email sent to an external organisation is written carefully before sending, in the same way as a letter written on academy headed paper.
- The forwarding of chain letters is not permitted in the academy.
- All email users to adhere to the generally accepted rules of online etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication or arranging to meet anyone without specific permission.
- Pupils immediately tell a teacher/ trusted adult if they receive an offensive message and keep a copy of it as evidence.
- Staff must inform the Online Safety Coordinator (**Claire Quinn**) if they receive an offensive email or message.

Safe use of Images/ Video taking of images and video

Digital images/video are easy to capture, reproduce and publish and, therefore, easily 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 staff, the academy permits the appropriate taking of images/ video by staff and pupils with academy equipment (iPads).
- Staff are not permitted to use personal devices (mobile phones, tablets or cameras) to record images of pupils, including when on field trips. However, with the express permission of the Executive Principal, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the staff device.

Consent of adults who work at the academy

- Permission to use images/video of all staff who work at the academy is sought on a regular basis and a copy is located in the personnel file and in the "Consent file" held by the Local Compliance Officer (LCO)located in SLT office.

- Parents must seek permission to take photos/video academy events, and must agree to NOT post images/video on the internet.

Publishing pupil's images and work

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

- on the academy website
- on the academy blog/twitter-feed
- in the academy prospectus and other printed publications that the academy may produce for promotional purposes
- 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, ie exhibition promoting the academy
- general media appearances, eg 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 period that the child attends this academy unless there is a change in the child's circumstances where consent could be an issue (eg divorce of parents, custody issues etc) Parents/carers may withdraw consent at any time. Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils are not published online. Pupils' full names will not be published.

- Before posting student work on the internet, staffcheck to ensure that permission has been given for work to be published online.

Storage of Images/Video

- Images/video of children are stored on the academy's network and the online Google Drive.
- Rights of access to this material is restricted to the teaching staff and pupils within the confines of the academy network.
- Images / video of pupils are deleted where possible when pupils leave the academy and if consent to use these images/videos has been withdrawn.
- The network manager (**Peter Mason**) has the responsibility of deleting the images when possible when specified.
- The Local Compliance Officer ensures that any withdrawal of consent is actioned and logged.

CCTV

- CCTV is used in the following areas: outside.
- The academy uses CCTV for security and safety. The only people with access to this is the Site Manager and Network Manager (**Kelvin Kay**). Notification of CCTV use is displayed at the front of the academy.

Misuse and Infringements

Complaints

Complaints relating to Online Safety are made to the Online Safety Coordinator and Designated Safeguarding Lead (**Claire Quinn**). Incidents are logged and processes in line with Academy policy are followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach is immediately

reported to the Online Safety Coordinator (**Claire Quinn**) and the Network Manager (**Peter Mason**).

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Coordinator (**Claire Quinn**) and the Network Manager (**Peter Mason**), and may lead to:
    -
    - Investigation by the Executive Principal
    - Immediate suspension
    - Dismissal
    - Position of Trust/ LADO referral
    - Involvement of police

Equal Opportunities

The academy endeavours work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the academy's rules

Pupils with additional needs

.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

Parental Involvement

- We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of academy while appreciating the benefits provided by technologies generally.
- We regularly consult and discuss with parents/carers and seek to promote a wide understanding about the link between technology and safeguarding.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on induction to academy.
- 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 (eg on academy website, blog or twitter-feed)

Reviewing this Policy

Review Procedure

There is an ongoing opportunity for staff to discuss with the coordinator any issue of Online Safety that concerns them.

This policy is reviewed every 12 months or before 12 months if required,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, Executive Principal and governors on October 2018

To be reviewed: September 2019