IT Code of conduct and Acceptable use policy

Primary and Secondary Academies

September 2017

ChatPol / ALL / 0048 / 1709a

Policy links
This policy should be read alongside the CHAT *e-safety policy* which can be found on the academy website.

Introduction

All academies hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could, if not processed securely, be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the academies. This can make it more difficult for Cuckoo Hall Academies Trust to use technology to benefit learners.

As such, all members of staff have a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Staff also have a duty to take proper care of any equipment issued to them

The acceptable use agreement (See **APPENDIX 2**) should be issued to the appropriate user for signature, collated by a designated member of staff and returned to Human Resources.

Monitoring

All internet activity is logged by the school's internet provider

If authorised to do so, Information and Communications Technology (ICT) staff may:-

- inspect any ICT equipment owned, hired or leased by the school at any time without prior notice.
- monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet / intranet use and any other electronic communications (data, voice or image) involving its employees or contractors without their consent, to the extent permitted by law. (Please see **APPENDIX 1**)

This may be to:-

- confirm or obtain information for business continuity (for example where someone's absence significantly impedes business continuity);
- confirm or investigate compliance with Trust policies, standards and procedures;
- ensure the effective operation of school ICT;
- comply with a Subject Access Request under the Data Protection Act 1998
- to prevent or detect crime.

If staff are in doubt as to whether the individual requesting such access is permitted to do so, they may contact a member of the Senior Management Team for verification.

Authorisation for ICT to act with regard to the above will require justification for doing so agreed in writing as follows:-

- Staff — Written justification from both the Chief Executive Officer and a member of the Senior Management Team (SMT)
- SMT Staff — Written justification from both the Chief Executive Officer and a Trustee
- CEO — Written justification from both the Chair of the Board of Trustees and another Trustee

Breaches

For staff, any policy breach is grounds for disciplinary action in accordance with Cuckoo Hall Academies Trust Disciplinary Procedure. Depending on the severity, policy breaches may also lead to criminal or civil proceedings.

A breach or suspected breach of policy by an academy employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

How we process and handle personal data is governed by the Data Protection legislation which is in turn regulated by the Information Commissioner (ICO). The legislation empowers the ICO with a number of tools for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. These include audit, criminal prosecution, non-criminal enforcement and the power to serve a significant monetary penalty notice on any organisation that causes a serious breach of the Data Protection law.

Data Protection legislation also enables the ICO to:

- serve information notices requiring organisations to provide them with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and ‘stop now’ orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.

E-mail

The use of email within our academies is an essential means of communication for both staff and pupils. In the context of an academy, email should not be considered fully private. Educationally, email can offer significant benefits including direct written contact within an academy, between academies, national or international (be they staff based or pupil based).

Managing e-mail

Via access to its network via an individual profile, Cuckoo Hall Academies Trust provides most staff with their own email account to use for all school business as a work based tool. This is to protect staff, 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 all their passwords secure.
- For the safety and security of users and recipients, all email is filtered and logged; if necessary email histories can be traced. The academy email account should be the account that is used for all academy business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Our academies require a standard disclaimer to be attached to all e-mail correspondence stating that, '*The views expressed are not necessarily those of the school or Cuckoo Hall Academies Trust*' or similar and this will be enforced by the ICT department.
- All e-mails should be written and checked carefully before sending, and care should be given to those being sent external to the organisation in the same way one would check a letter written on academy headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to carbon copy (cc) the headteacher, line manager or designated account.
- Pupils should only use academy approved accounts on the academy system and only under direct teacher supervision for educational purposes.
- Emails created or received as part of an academy job are subject to disclosure in response to a request for personal data under the subject access provisions of the Data Protection Act 1998 or in response to a request for information under either the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

  Staff should therefore actively manage your e-mail account as follows:

  - Delete all emails of short-term value
  - Organise emails (e.g. into folders) and carry out frequent house-keeping on all folders and archives
  - Pupils encouraged to use a class / group e-mail address where agreed with the headteacher.

- All email users are expected to adhere to the generally accepted rules of net etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.
- Email attachments should be virus checked.
- Staff must inform their headteacher / line manager if they receive an offensive email
- However you access your academy email (whether directly, through webmail when away from the office or on either academy or non-academy hardware), the academy email policy applies

Sending emails (general)

- Use your own academy email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to a shared folder rather than sending attachments.
- Academy email is not to be used for personal advertising.

Receiving emails

- Emails should be checked regularly
- Staff should activate their '*out of office*' notification when away for extended periods and include a message that informs others when they are likely to return and who they may contact in their absence.
- Attachments from an untrusted source should never be opened. The IT department can be contacted for advice if anyone is unsure.
- Email accounts should not be used to store document attachments. If required, these should be detached and saved to the appropriate network folder
- The automatic forwarding and deletion of emails is not permitted.

Emails containing personal, sensitive, confidential or classified information

Where it is concluded that email must be used to transmit such data:

- Express consent should be obtained from the line manager to provide the information by email.
- Information should not be sent to any recipient if it has not been possible to accurately verify their details (usually by phone).
- The subject line of the email should not be used to identify such information.

- Encrypt the email and / or password protect the attachments. A password should be provided by separate method of contact with the recipient.
- The email should not be copied or forwarded to any more recipients than is absolutely necessary
- Confirmation of safe receipt should be requested.
- In exceptional circumstances provision can be made for communication with other external agencies.

Passwords and password security

Passwords

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon i.e. do not include passwords in any automated logon procedures
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols in order to make it difficult for others to guess.
- Staff should:-
    - Change their temporary passwords at first logon
    - Only disclose their personal password to authorised ICT support staff when necessary **and never to anyone else**. On those occasions, staff should ensure all personal passwords that have been disclosed are changed once the requirement for that disclosure is complete.
    - **Never tell a child or colleague their password**
    - **Immediately inform the head of IT should they be aware of a breach of security with their password or account**

Password security

- Password security is essential for staff, particularly as they are able to access and use pupil data.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school 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 any workstations which are left unattended are locked.
- Due consideration should be given when logging into the school learning platform, virtual

learning environment or other online application to the browser / cache options (shared or private computer)

- In our academies, all ICT password policies are the responsibility of Head of information Technology and all staff and pupils are expected to comply with the policies at all times
- IT will ensure that systems enforce regular changes to generic passwords to reduce the risk of any unauthorised access

Internet access

The internet is an open worldwide communication medium, available to everyone 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 the **Grid for Learning** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Whilst internet use is covered in more detail within CHAT's *e-safety policy*, it should also be noted that:-

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials (including both text and images) from electronic resources
- On-line gambling or gaming is not allowed
- Our academies also employ some additional web-filtering which is the responsibility of the Head of IT.
- Staff and pupils should be aware that school based email and internet activity can be monitored and explored further if required
- CHAT academies are aware of their 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
- The academies do not allow pupils access to internet logs
- The academies may use management control tools for controlling and monitoring workstations

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Head of Information Technology, the Head of Facilities Management and appropriate

members of the Senior Leadership Team.

- Notification of CCTV use is displayed in the academies.
- We do not use publicly accessible webcams in the academies
- Webcams in school are only ever used for specific learning purposes and never using images of children or adults
- Misuse of the webcam by another member of the school community will result in sanctions

Equipment security

This section covers such items as desktop PCs, laptops, tablets, mobile devices and removable data storage devices including the software.

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager.
- Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their unit
  - recovering and returning equipment when no longer needed
- The IT department will log equipment issued to staff and record serial numbers as part of the school's inventory
- Users of academy ICT equipment are responsible for their activity
- Users must ensure that all ICT equipment is kept physically secure at all times whether onsite or in transit. Portable equipment must be transported in its protective case if supplied
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Users must not attempt unauthorised access or make unauthorised modifications to computer equipment.
- The loss or theft of any equipment must be reported **immediately**.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Software and data security

- It is imperative that data is frequently saved on to the academies network.

- Visitors must not connect their privately owned own ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.

- All school data should be stored on the school network. Personal or sensitive data should not be stored on the local drives of a desktop PC / laptop, USB memory stick, or other portable device.

  If it is necessary to do so the local drive or portable device must be encrypted. Users will be responsible for the backup and restoration of any of their data that is not held on the academies network. All locally stored data, including diary entries, should be synchronized with the central school network server on a frequent basis.

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

- Where the school provides mobile technologies such as phones, laptops and iPads for staff, only these devices may be used to conduct school business outside of school.

- Users must 'lock' their device (for desktops and lap tops via the CTRL + ALT + DEL keys) if leaving it unattended to prevent unauthorized access to personal data. It is recommended that a time locking screensaver is also applied to all machines.

- It is users responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person either on or offline.

- Users must not attempt unauthorised access or make unauthorised modifications to computer, programs, files or data. This is an offence under the Computer Misuse Act 1990

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support unless otherwise instructed.

Computer Viruses

It is the responsibility of the academies, by delegation to the IT department, to ensure that anti-virus protection is installed and kept up-to-date on all academy machines.

All files downloaded from the internet, received via e-mail or on removable media (such as a memory stick) must be checked for any viruses before use by anti-virus software approved by Cuckoo Hall Academies Trust.

- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
- Anyone using personal removable media is 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 responsibility of Cuckoo Hall Academies Trust to install or maintain virus protection on personal systems.
- Class teacher must arrange for IT to first perform a safety assessment first if pupils wish to bring in work on removable media.
- No one is permitted to download programs onto on school based technologies without seeking prior permission from the IT department.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and report it to the IT department immediately. They will advise you what actions to take and be responsible for advising others that need to know.

Leavers

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

On termination of employment or resignation all ICT equipment must be returned to the line manager along with details of all system logons so that they can be disabled.

Once notified of their departure, the IT department will ensure that:-

- user ID and passwords for staff and pupils who have left the school are removed from systems as soon as practicable and within 48 hours
- all user accounts are disabled once a member of staff has left
- prompt action is taken in disabling accounts to prevent unauthorised access

Mobile phones

Mobile phone use is covered by the sections 'Equipment security' and 'Software and data security' above and expanded further in the sections below however in any event,

It is not acceptable for staff to have a mobile phone switched on during lessons and, aside from members of the Trust's Senior Leadership Team, it is not acceptable for staff to talk on phones whilst walking around the school building during the normal school day.

Trust provided mobile phones

- The sending of inappropriate text messages between any member of the school

community is not allowed

- Permission must be sought before any image or sound recordings of any member of the school community are made on the devices
- Users are responsible for the security of their school mobile phone. The PIN code must always be set.
- Users must not leave their phones unattended or on display (especially in vehicles). The school remains responsible for all call costs until the phone is reported lost or stolen
- Users must read and understand the instructions and safety points relating to the use of their school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK without the permission of the Chief Executive Officer or Executive Headteacher
- Users must not send text messages to premium rate services
- In accordance with the **Finance policy** on the private use of school provided mobiles, users must reimburse the school for the cost of any personal use of their school mobile phone including call charges incurred for incoming calls whilst abroad. Adding an asterisk symbol [*] to the end of the number being contacted assists in identifying personal use numbers as these will be shown separately on a bill. Payment arrangements should be made through via the finance department.

Personal mobile phones

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Under no circumstances are staff permitted to contact a pupil or parent / carer using their personal device
- Personal mobiles should never be used to take photographs, video or recordings of children.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Bluetooth, NFC or other peer-to-peer radio communications should be hidden / switched off
- The Trust is not responsible for the loss, damage or theft of any personal mobile device

Incident reporting

Any of the following must be reported to CHAT's Head of Information Technology.

- Any suspected, attempted or actual security breaches
- Unauthorised use or suspected misuse of ICT
- Loss, theft or suspected theft of equipment
- Lost / stolen data* (including any remote access Secure ID tokens and PINs)
- Unauthorised use of ICT
- Suspected, attempted or actual misuse of ICT
- Virus notifications
- Unsolicited emails
- Any other policy non-compliance

Depending on the nature of the incident, the Safeguarding Manager may also need to be notified. (*****Any loss of data and the specifics must also be reported to the Governance Manager immediately).

Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence, an investigation by the Headteacher or their nominee, immediate suspension, possible dismissal in line with HR policies and procedures and involvement of police for very serious offences.

Legislation relating to monitoring of staff email, e-safety and the protection of personal data

Data Protection Act 1998

The Data Protection Act requires anyone or any organisation who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. RIPA was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Human Rights Act 1998

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing threatening written material is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) or arranged to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18 with who they are in a position of trust.

Communications Act 2003 (Section 127)

A person sending a message or other matter that is grossly offensive or of an indecent, obscene or menacing character by means of the Internet; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (Sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (Section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (Sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Freedom of Information Act 2000

Environmental Information Regulations 2004

	ICT Acceptable Use Agreement

Information and communications technology (ICT) including data and related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life.

This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents in conjunction with our e-safety policy and IT code of conduct and acceptable use policy. Any concerns or clarification should be discussed with your line manager as appropriate.

I will:

- only use CHAT email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the CHAT Board;
- comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities;
- ensure that all electronic communications with pupils and staff are compatible with my professional role;
- ensure that any personal data is kept secure and is used appropriately, whether in CHAT premises or accessed remotely. Personal data should never be taken off premises outside of the CHAT network without explicit written authorisation of the Headteacher / Chief Executive Officer and must always be encrypted. Hard copies of personal data should never be taken off site;
- ensure that images of pupils and / or staff will only be taken, stored and used for professional purposes in line with CHAT policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the CHAT network without the explicit permission of the parent / carer;
- support the academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the CHAT community;
- respect copyright and intellectual property rights;
- ensure that my online activity, both in and outside school, will not bring my professional role or the Trust into disrepute; and
- support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I will not:

- give out my own personal details, such as mobile phone number and personal e-mail address, to pupils;
- use my personal email for any CHAT related business;
- install any hardware or software on CHAT equipment without the permission of the Head of Information Technology;
- browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;
- connect my privately owned own ICT hardware to the CHAT network.

I understand that all my use of the internet and other related technologies can be monitored and logged and understand that this forms part of the terms and conditions set out in my contract of employment (where employed).

I understand that I am responsible for all CHAT IT assets ('asset') which are given to me including, but not restricted to, laptops, mobiles and tablets. I must act reasonably and take appropriate measures to prevent losses arising from wilful action by others, both outside and within the trust, which may result in the damage, theft, loss, abuse or unauthorised access to assets. If I am deemed to have intentionally omitted or committed a wrongful act or negligence that caused the loss or damage of an asset, I understand that I will be liable for the loss or damage up to the market value of the asset and this will be deducted from my pay. Furthermore, upon cessation of employment with CHAT, if an asset is not returned, I will be liable to cover the market value of the asset and this will also be deducted from my pay.

✂

Acceptable Use Agreement

I have read, understood and agree to adhere to the CHAT IT Code of conduct and acceptable use policy, supporting the safe and secure use of ICT throughout Cuckoo Hall Academies Trust.

Name .....

Signature .....

Job title / role .....

Date .....