ICT and e-Safety Policy

1 GREAT ACADEMIES STATEMENT OF INTENT

Great Academies Education Trust understands the positive contribution ICT can make to our working and learning environment but is equally aware of the dangers and risks associated with its use.
This Policy aims to outline the procedures for the responsible use of ICT, including the internet, and supplements the Academy's wider role in safeguarding and promoting student welfare. The term 'internet' is used to cover the worldwide web, and all e-communication such as e-mail and social media.

Creating a safe ICT learning environment includes three main elements at GAET academies:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities for monitoring the use of ICT;
- A comprehensive e-Safety education programme for students, staff and parents.

This policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the schools and the policy will not remain static. It may be that staff and pupils might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

2 OUR AIMS

To use a range of appropriate and up to date technologies to

- aid teaching and learning;
- ensure smooth running of school operation including storage and maintenance of records, payment and ordering systems, biometric systems, site, staff and pupil security;
- aid communication with parents.

3 OBJECTIVES

This policy is designed to

- ensure appropriate and safe use of equipment including mobile devices
- support staff and pupils with the safe use of internet and e-mail

- provide guidance to staff on the appropriate use of social media
- describe how an academy website should be used and maintained
- remind staff of copyright legislation
- support staff with the appropriate use of imagery, including CCTV and video applications.

4 IMPLEMENTATION GUIDANCE

This policy applies to all staff and governors, and it also applies to supply staff, volunteers, student teachers, people on placement, visitors and any other person working in the Academy who has access to Academy systems. It also applies to pupils and their parents/carers and to anyone accessing ICT within the school building or using ICT to communicate with teachers.
The policy covers all electronic devices, including laptops, PCs, tablets and mobile phones and emerging technologies.
Failure to comply with any part of this policy may result in action under the disciplinary procedure or other appropriate action being taken.

4.1 Appropriate and safe use of equipment

Staff and pupils must treat with respect equipment in school and at other sites accessed through school, and are subject to regulations imposed by the respective service providers. Students should be aware of the school rules and how they relate to the use of ICT equipment.

4.1.1 School equipment

Inventory , signing out, recall of equipment, safe storage, disposal
Each GAET academy will keep centrally a full list of all ICT equipment held by the school, including that held by individual year groups or departments. There will be a clear procedure for signing out equipment to staff and pupils, and for its return.
Safe and secure storage arrangements must in place when equipment is not in use.
When equipment is disposed of, the data must be removed from memories or the equipment reformatted and where equipment is recycled, this must be with certified recycling centres, in line with Waste Electrical and Electronic Equipment (WEEE) recycling and evidence retained.

Desktops, laptops, netbooks, tablets and educational equipment
Staff and pupils will use a range of appropriate technologies to support teaching and learning. Staff will be supported in the use of the technologies and pupils should be appropriately supervised and taught the skills to use specific equipment required.

Storage devices
The use of external storage devices such as USB drives, external hard drives etc. is determined by each GAET academy. If the use of these devices is permitted, it must be in line with the academy's procedures.

School mobile phones
For events such as school trips and sporting events, a school mobile phone may be available to staff. This must be used for all communications during the events, staff personal phones must not be used without prior agreement with the Principal or Educational Visits Coordinator. Personal mobile phone numbers should not be shared with parents/carers or pupils unless in exceptional circumstances such as a staff member being a parent of a pupil at the school and agreed by the principal or Designated Safeguarding Lead.

Cameras, video cameras, webcams and related software/applications
These must be used in line with the Trust's Safeguarding and Child Protection Policy.

- Permission is obtained from a child's parent or carer at admission, before photographs or video footage can be taken, and a central record maintained**.** Those refusing to give permission will be recorded and teachers must verify class lists prior to an event. This permission is for the full time the pupil is on roll at the academy; parents may in writing revoke this permission at any time.
- If staff need to use their own devices to record images, then these photographs or video footage will be downloaded as soon as is reasonably possible to a staff area and saved into a designated folder, and deleted from the device and its cloud memory.
- Any photographs or video footage stored after the pupil(s) have left school will be deleted if no longer needed or archived on the school network only.
- For school trips or visits, school cameras, video cameras or camera phones should be used where possible.
- Webcams must not be used for personal communication and should only be used with an adult present.
- Pupils and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

CCTV
CCTV must only be used in line with Information Commissioner's Office (ICO) CCTV Code of Practice and the Data Protection Act 1998. It must be used responsibly in order to safeguard both trust and confidence in its use.
The CCTV system is owned by GAET and operated by the academy, the deployment of which is determined by the academy's leadership team.
The planning and design must endeavour to ensure that the scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the

system will cover or detect every single incident taking place in the areas of coverage.
The CCTV can be monitored centrally from the academy by a named person, in line with ICO guidance.
CCTV warning signs will be clearly and prominently placed at all external entrances to the academy, including academy gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the academy will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

Siting the Cameras

- The system may comprise a number of fixed and dome cameras.
- Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The academy will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.
- The academy will make every effort to position cameras so that their coverage is restricted to the academy premises, which may include outdoor areas.
- CCTV may occasionally be used in classrooms for the purpose of protection of costly equipment. This must be with the full awareness and permission of staff operating in those areas. It may also be used in areas within the academy that have been identified by staff and pupils as not being easily monitored.
- Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring (see below).

Covert Monitoring

The academy may in exceptional circumstances set up covert monitoring. For example:
i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.
In these circumstances authorisation must be obtained from the principal or Chair of Governors.
Covert monitoring must cease following completion of an investigation.
Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
All retained data will be stored securely.

Access to CCTV images
Access to recorded images will be restricted to those persons authorised to view them, and will not be made more widely available.
A record will be kept of all occasions when CCTV imagery is viewed, which must include the date and time of the footage, the persons whose images were viewed, the persons viewing and the reasons for doing so.

Subject Access Requests (SAR)
See Trust Data protection policy

Access to and Disclosure of Images to Third Parties
There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).
Requests should be made in writing to the Principal.
The data may be used within the academy's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Classroom video use

The academy may use video camera systems such as IRIS Connect in classrooms to support the development of teaching expertise through self-reflection, enquiry, building teacher learning communities and coaching. Such systems are not surveillance system; they are permission-based with multiple levels of security to ensure that teachers can feel confident and empowered remain in control throughout the process.

If the school makes use of this technology, it must be in line with the relevant guidance from the Information Commissioners Office (ICO). It is the responsibility of the principal to ensure parents are appropriately informed and relevant permissions are gained. These permissions gained do not provide any rights to parents or pupils to access information stored on other individual user accounts.
The privacy rights of users must be paramount and they must remain in full control of any video from beginning to end of the process, including deletion of footage.
There must be no system 'override' to give administrator rights to remotely or subsequently view a lesson without the permission of the teacher.
All staff using the system will be trained appropriately. Where a user decides to agree to share the information, the system will be used confidentially, sensitively and developmentally and with due respect for colleagues;

4.1.2 Protecting equipment and data

School network

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- GAET academies will work in partnership with LAs, external provider companies, DfE and the internet service providers to ensure systems to protect students are reviewed and improved.
- All users are asked to respect the privacy of files of other users. Staff should not access other members of staff's individual drives. Staff will need to access pupils' work e.g. for marking, or retrieval, and pupils should understand that this is the case. Pupils should not enter file areas of other users. All users are reminded that files to be shared should be saved to the shared areas available.
- There are occasions where it will be necessary for a member of staff e.g. a network manager, to access a member of staff's individual drive or email. This might be because a staff member is off site and cannot get full access, is on sick leave. This access will only occur with
  (a) the permission of the member of staff concerned or with prior notification,
  (b) for purposes of investigations under the Trust's discipline policy, under the instruction of the relevant senior leader, chair of governors or Trust officer.

  There must be no routine monitoring of individuals' activity unless this has been communicated clearly. An example of appropriate use would be the remote monitoring of pupils' work in an ICT suite, where the pupils know this can be done. There must be no routine monitoring of staff activity, neither should CCTV be routinely viewed.

  There may be occasions where a member of staff e.g. a network manager, needs to access a member of staff's individual drive or email for the purposes of investigation into a disciplinary or criminal matter. This must occur in line with the Trust's policies and/or relevant legislation.
- All users accessing software or any services available through the school network must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. All users should be aware that some items are licensed for educational or restricted use only.
- All users are expected to be responsible for their own areas on the school network.

Passwords and anti-virus/malware protection

- Passwords must be set for each user.
- Passwords should be a minimum of 7 characters and must contain letters, numbers & special Characters such as *&^%$. They should not contain spaces
- Passwords must not be shared with other users.
- Staff passwords must be changed regularly. (maximum password lifetime 180 days)

- Users requiring assistance in changing their password should contact the ICT technical staff.
- The school's instructions to update anti-virus/malware on any devices must be followed

Personal and sensitive data

- All staff must log off or lock computers when they leave any room including when using the school systems at home.
- No sensitive or personal information must be displayed on whiteboards when classes are present.
- Staff must also take care when working remotely that no personal or sensitive data could be viewed by unauthorised persons e.g. family members on shared home computers.
- No unprotected storage devices such as USB drives or external hard disc drives are to be used to store sensitive or personal information, they must be owned by the school and encrypted. This includes lists of pupils' names, school reports.
- Each academy must ensure that staff have levels of access to sensitive information as appropriate to their roles and responsibilities. eg access to SIMS (MIS), exam board data, CP information.
- Biometric data must be used in line with relevant legislation and the Trust's data protection policy.

System and data back-ups

- Each academy must have in place sufficient and appropriate systems for system and data back-ups to ensure that any information lost can be recovered. Backed up data must be held in a different building from the main back-up location, and this should normally be an officially agreed location such as another appropriate building on the school campus, another Trust school or the Sponsor's HQ.
- Data must be held in line with legislation, including for LAC and pupils with SEND.

Acceptable use agreements (AUAs)

All staff, pupils and ICT contractors/suppliers must read and sign the appropriate acceptable use agreements (see appendices).

Each academy must retain copies of the acceptable use agreements for the period of the member of staff's employment or the pupil's time on the school roll. Contractor/supplier AUA documents should be retained indefinitely.

Disposal of ICT equipment

Items which appear on the IT inventory must not be disposed of without first obtaining permission from the principal or member of staff to whom this decision is delegated. Items must not be physically removed from their normal locations except under the supervision or at the direction of the IT support staff.

Equipment which is replaced by newer items will generally be re-used elsewhere where it is reasonably possible to do so. If complete units cannot be re-used, components will be re-used or kept for spares.

Equipment will generally only be disposed of if it meets one of the following criteria:

- it is damaged or broken beyond reasonable or economic repair,
- it no longer meets relevant Health and Safety or operating standards and cannot economically be modified to do so,
- it is no longer fit for purpose and it cannot be re-used for another purpose elsewhere.

Consideration should be given to passing on working and safe equipment to others who might be able to make use of it; disposal to waste or re-cycling will be used only as a last resort.

Arrangements should be made with the site management team for the disposal to waste or approved re-cycling of equipment. This must be to an approved disposal centre.

No electrical and electronic items should be disposed of in the general waste if they come within the scope of the WEEE regulations and must only be disposed of in an approved manner. Computers and other equipment containing data discs should not be disposed of until all sensitive data has been removed or the physical medium rendered unreadable. If a computer is to leave the school in working condition all software for which a licence is required and which is not transferable with the device under the licence conditions should also be removed.

Discs and Data Storage devices or media which are to be disposed of which may have contained personal or sensitive data, for example server or SAN disks, should be physically destroyed before being sent to waste disposal.

On disposal, the item must be removed from the inventory.

4.1.3 Staff and pupils' own devices including mobile phones

Staff mobiles and own devices
Mobile phones are widely used and easily accessible and therefore specific caution should be used with these devices. During work time, personal mobile phones should only be used for legitimate work purposes. Personal use should be restricted to break times.

Pupil mobiles and own devices (Bring Your Own Device - BYOD)

Students may be allowed to bring mobile devices into the Academy. The academy appendix will say if this is so. If the use of a personal mobile device is allowed by the school, and pupils choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

- Use of the device during lesson time will only be allowed with the agreement of the teacher and for the explicit purpose of supporting learning. Misuse of this privilege (using the device for a non-curriculum purpose or any unacceptable use) will result in the withdrawal of the privilege and may also result in the confiscation of the device.
- If the use of a device has not been specified by the teacher then it must be kept out of sight during lessons and switched to silence or off.
- Devices must not be used during lesson change and must be kept out of sight.
- No student may take a mobile phone or other 'smart' device into a room or other area where examinations are being held.
- The security of devices will remain the student's responsibility in all lessons including PE/sports lessons.
- The Academy will not be held responsible for any damage incurred to a student's mobile device.
- The Academy is not responsible for any costs incurred by students whilst using their own device.
- Students will not have access to the Academy's wireless network and should not make any attempts to access it.
- Students are not permitted to use the Academy's facilities to charge their mobile devices.
- Mobile devices will not be used during a controlled assessment or any external examination unless the examination board has clearly permitted their use.
- If requested, content on the device (e.g. messages, emails, pictures, videos, sound files) must be shown to a designated teacher.
- The Academy's acceptable use agreement is applicable on the use of personal mobile devices by students.
- The Academy's Internet filtering is not applicable on students' devices. Therefore, any Internet use, on Academy premises, through mobile phones is the responsibility of students and parents/carers and is subject to the Academy's acceptable use agreement.
- In accordance with the Academy's safeguarding policy, students must not use their mobile devices to make contact with any individual or group outside the Academy, or take photographs, during school time.

4.2 Safe use of internet, email and social media

Internet

Staff and pupils alike should adopt a critical awareness of validity of content on the internet. They should only access websites needed for their work or learning. They should be aware that the school has appropriate monitoring, filtering and alert

systems which will alert technical staff of any attempts to access inappropriate material, and that this access will be reported and followed up as appropriate. If staff or students accidentally access an unsuitable site, it must be reported to the relevant school staff, for example the designated safeguarding lead, e-Safety Co-ordinators or the Network Manager.

It is the role of staff to understand the issues of key risks posed to young people through the internet, including grooming and radicalisation. Staff should be able to able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns.

Considerate use of the internet

The following general principles should be adopted:

- All communications should be polite and users should seek to ensure their communications such as emails could not be interpreted otherwise.
- Appropriate language should be used in all communications as is fitting to a representative of the school, using a non-private network. This includes social media at any point.
- Disruption of the use of the internet by other users should be avoided: e.g. downloading large files or video streaming during lesson times and other high volume activities.
- E-mail congestion should be avoided, for example e-mails should not be copied to those who do not need to see them.

E-mail

Whenever e-mail is sent using your school account, the sender's name, job title, e-mail address and the school's name must be included.

- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- If you receive e-mail from outside the school that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the school's guidelines).
- You should be aware that, in the event of the school being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Staff accessing email on personal devices to access school emails, you will need to ensure that your device is secured by a password/code at all times, that this is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

Staff use of social media, personal devices and e-mail

- Use social media with care. The use the maximum security settings available is strongly recommended. Seek advice if you require assistance in setting up security settings.
- You should never accept students as 'friends' when using social media. You should also be wary of accepting former students, especially if they have younger siblings still at school. Best practice guidance is that students must have left the school for a minimum of three years and be over 19 before they can be accepted as friends. You should also exercise caution if you have parents as 'friends'.
    - If there are exceptional circumstances, eg you have a relative at the school who is linked to you on social media, you must follow the school's procedure for recording this.
- You should not communicate with students or parents via personal email nor should you provide any students with your personal contact details including mobile telephones.
- Students and former students up to the age of 19 are protected under safeguarding procedures and staff should ensure they do not leave themselves vulnerable under these procedures.
- Inappropriate discussion about staff, students or the Academy in general, or discussion which might have a detrimental impact on the reputation of the Academy is strictly forbidden and may result in disciplinary action.

Cyber bullying

See GAET Anti-bullying policy

Youth-produced sexual imagery (Sexting)

This is the sending of sexually explicit digital images, videos, text messages, or emails, usually by mobile phone. In cases which come to the attention of the school, these should be dealt with in accordance with the Trust's safeguarding policy and UKCCIS guidance.

Looked after children

LAC - Students who are looked after, or have formerly been looked after, may discuss e-contact with you that has been made with them by their birth families. Always report this to the designated person for LAC in school, who will contact the child's foster carers and social worker.

- Assure student that they have done nothing wrong
- Collate all evidence
- Pass the information to the designated person, who will pass the information to Social Worker and Foster Parents or Adoptive Parents.
- Offer e-safety training to foster family and young person if required

Personal Use of Academy Email and Internet
The personal use of e-mail and or internet is a privilege and not a right, and inappropriate use will result in the cancellation of the privilege and may lead to disciplinary action being taken against you, including dismissal.
The Academy e-mail system is primarily for business use. Occasional and reasonable personal use is permitted provided that this does not interfere with the performance of your duties.

Cloud storage
Any storage of data to 'cloud' locations must be in line with 'Cloud computing: how schools can move services to the cloud' DfE 2016.

4.3 The academy website and other e-communication methods

The academy must have a limited number of named persons with responsibility for upkeep of the school's website, blogs and social media feeds. The website should be kept up to date and should undergo annual review. The school must abide by the GAET Safeguarding policy and the instructions of parents/carers regarding the publication of pupils' photographs. Photographs should not be linked to individual pupils' names. The website must contain all material required by the DfE and should include e-safety sections for parents and pupils.

4.4 Copyright
The owner of copyright has the exclusive right in certain works such as documents, articles, books, plays and musical compositions, so that they cannot be copied or used in certain other ways without the consent of the copyright owner.
There may be certain licenses in place within the Academy which allow some materials to be copied. Staff and pupils must abide by copyright legislation and guidance.

Unauthorised use of copyright material may result in the owner of the material suing both the Academy and the individual member of staff for damages so it is important that staff are familiar with what they can and cannot use as teaching material. Copyright is easily infringed unintentionally when material is down downloaded from the internet, or when text is copied or attached to an email.

4.5 Data protection and freedom of information

These are covered by the Trust's polices on data protection and freedom of information.

4.6 Disciplinary and legal action

Any misuse of equipment or the internet either in school or outside of school which could constitute misconduct, gross misconduct or criminal activity will be investigated under the appropriate Trust policies and/or legislation.

4.7 Training

Academies will ensure training is provided as appropriate to staff members' roles and responsibilities. This may include:

- Basic use of available technologies and software/systems
- ICT security
- Data protection including security breaches
- Freedom of information
- Information security
- Records management
- Copyright
- Acceptable use of ICT
- E-safety
- CCTV

5. ROLES AND RESPONSIBILITIES

All persons to whom this policy applies must comply with it and with the school's related procedures. They must report any suspected misuse of ICT or other related concerns through the appropriate channels.

GAET
Ensures:

- policy implementation and review,
- monitoring of data breaches.

Local Governing Body
Ensures:

- policy implementation and review,
- there is a nominated trained governor (e-safety),
- there is monitoring of data breaches,
- a staff training record is kept.

Principal
Is responsible for:

- compliance with policy and school procedures,
- line management of ICT lead and/or system administrator,
- content of school website, blogs and social media feeds,
- deployment of CCTV.

Where these roles are delegated, the principal must maintain oversight and be assured that appropriate monitoring and evaluation is in place.

ICT lead
Takes the operational lead on:

- ICT curriculum,
- e-safety

and may line manage the system administrator

Members of staff with responsibility for CCTV
Are responsible for:

- ensuring policy and ICO guidance is implemented, and that robust record keeping is in place.

System administrator and technical staff
Are responsible for:

- procurement and disposal of ICT equipment with relevant permissions,
- maintenance of the school equipment and network,
- ensuring relevant filtering and alert systems are in place.

All teaching and support staff
Are expected to:

- provide and/or participate in training;
- support and contribute to a specific curriculum approach to safety, including issues of personal safety, self-esteem, bullying - including cyber bullying and prejudice based bullying, sex & relationships education, domestic abuse, child sexual exploitation, radicalisation, honour-based violence and forced marriage.

Pupils
Are expected to:

- use ICT appropriately,
- know what inappropriate use is, and report it promptly.

Parents/Carers
Have a key role in

- supporting their children in the safe and appropriate use of ICT,
- alerting the school immediately if they are aware of improper access / Cyber-bullying / broken website links.

6 EQUALITY

The Great Academies Education Trust ensures that all pupils are safeguarded. We do not discriminate against anyone on the grounds of their sex, race, colour, religion, nationality, ethnic or national origins. This is line with the Equality Act 2010 and covers both direct and indirect discrimination.

7 MONITORING, EVALUATION AND REVIEW

This policy should be read in conjunction with;
ICO guidance
Cloud computing: how schools can move services to the cloud DfE 2016
Keeping children safe in education 2016

Sexting in schools and colleges UKCCIS August 2016
GAET Policies including

- Safeguarding and child protection policy
- Anti bullying policy
- Staff discipline policy
- Behaviour policy
- Data protection policy
- Freedom of information policy
- Privacy notice
- Curriculum policies including Sex and Relationships Education
- Dealing with allegations against staff policy
- Educational visits policy
- Record keeping policy
- Recruitment and Selection policy
- Whistleblowing policy

Date 10th July 2017

Date for next review July 2019

8 SOURCES CONSULTED

- Data Protection Act 1998
- Freedom of Information Act 2000
- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Cloud computing: how schools can move services to the cloud; DfE 2016
- Counter Terrorism and Security Act (2015)
- Prevent Duty Guidance (2015)

Appendix 1

ICT Acceptable Use Agreement (Pupil, Primary)

Introduction

In order for pupils at ……. to browse the Internet or make use of email and other technologies, we require each child (and their parent / carer) to indicate that they understand the importance of adhering to these strict rules:

Email

- I will only use the internet when I have permission and am supervised.
- I will only send emails to people that my teacher has approved.
- I understand that racist or bad language will not be tolerated and my emails will be polite at all times.
- I will not use email to bully another child or adult.

Personal Details

- I will not give out my address, home or mobile telephone number, photograph or school name and address on the internet or in an email.
- I will not give out personal details of another child or adult on the internet or in an email.

Internet Access

- I will tell my teacher straight away if I accidentally come across any unsuitable pictures or information on the internet or if anything makes me feel uncomfortable or upset.
- I will only use search engines or websites that have been chosen or approved by a teacher.
- I will not try to access any inappropriate websites, chat rooms, instant messaging or social networking sites in school.
- I will not download any files from the internet in school unless I have permission.
- I will not attempt to download any programs to the school network.

Other technologies

- I will not use my mobile phone during the normal school day.
- If I bring my mobile phone into school for any reason I will hand it straight to my teacher for safe keeping until the end of the day.
- I will not use the camera on a mobile phone to take photographs of people without their permission.
- I understand that any form of bullying by text message is unacceptable and will not be tolerated.

Declaration

Pupil

I understand the rules of this agreement and agree to follow them. If I break any of these rules, I understand that:

1. A letter may be sent home
2. I may not be permitted to use the Internet for a given amount of time
3. More serious action may be taken

Pupil Signature Date:

Parent / Carer

- I give permission for my child to use the Internet, email and other technologies in school.
- I understand that pupils will be held responsible for their own actions and agree to appropriate sanctions being imposed if rules are broken.
- I am aware that some materials on the internet may be offensive and accept the school's standard for my child to follow when selecting and sharing information and media.

Signed Parent / Carer Date

Appendix 2
ICT Acceptable use agreement (pupil, secondary)

Using ICT including email, the internet and mobile devices are an expected part of our daily working life in school. All pupils must be safe and responsible in their use of ICT and related technologies.

Equipment, network and security

- I will treat school ICT equipment carefully and not cause any damage to it.
- I will not share any passwords provided to me by the school.
- I will only access the computer system with the login and password I have been given.
- I will not access other network user's files.
- I will not connect a computer/laptop/Tablet to the network / Internet that does not belong to School.
- I will not download anything onto memory sticks or other devices without permission.
- I will not attempt to download any programs to the school network.

Internet

- I will only use the school's email / Internet / Intranet / Learning Platform as allowed by the school staff.
- I will not browse, download, upload or send material that could be considered offensive or illegal.
- I understand that all my use of the Internet can be monitored and logged by school staff.
- I will report any accidental or intentional access to inappropriate materials by staff or pupils.
- I will not allow anyone else to access my Email or files.
- I will not use social-networking websites (e.g. Snapchat, Instagram, Facebook etc.) using during lesson time.
- I understand I should not have school staff as my 'friends' on social-networking sites, unless there are exceptional circumstances, eg I have a relative at the school who is linked to me on social media.
- If I am worried about the e-safety of another pupil I will let a member of staff know
- I understand that racist or bad language will not be tolerated and my emails will be polite at all times.
- I will not use email to bully another child or adult.

Data

- I will not give out my address, home or mobile telephone number, photograph or school name and address on the internet or in an email.
- I will not give out personal details of another child or adult on the internet or in an email.
- I will not take pictures or videos of other people without their permission.

User Signature

I have read and understood this agreement. I understand that if I break the agreement the school will take action.

Signature

……

Date ……

Full Name ……..... (printed)

Appendix 3
Staff Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. All staff are expected to support and promote the Trust's ICT and e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

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. Any concerns or clarification should be discussed with the school e-Safety coordinator or ICT lead.
Failure to adhere to this agreement may result in disciplinary action in accordance with the Trust's ICT and e-safety policy.

Equipment, network and security

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given.
- I will not access other network user's files unless specifically authorized to do so.
- I will follow the school's instructions to update anti-virus/malware on any devices signed out to me.
- I will not connect a computer/laptop/Tablet to the network / Internet that does not belong to School or have up-to-date version of anti-virus software/anti-malware.
- I understand that if the school allows the use of storage devices, these must be encrypted.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will not attempt to download any programs to the school network.

Internet

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will not browse, download or upload material that could be considered offensive or illegal.

- I will not send to pupils or colleagues material that could be considered offensive or illegal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will report any accidental or intentional access to inappropriate materials by staff or pupils to the appropriate member of staff.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I will not use social-networking websites (e.g. Snapchat, Instagram, Facebook etc.) using Academy property during working hours. I understand access on my personal device should not be in lesson time or in view of any students.
- I understand I should not accept current or former students as 'friends' on social-networking sites until either of the following criteria have been met: Students have left Academy by a minimum of three years, or students are at least 19.
- If there are exceptional circumstances, eg I have a relative at the school who is linked to me on social media, I will inform the named person in school who will keep a record of this.
- I understand that if current students contact me via any electronic messaging like social networking sites, I must NOT accept the request and I must report the occurrence to the academy's designated safeguarding lead, with a copy of the contact.
- I recognise that radicalisation can occur to an individual from any section of society and is not particular to any racial, ethnic or social group. I further recognise that in many instances the process of radicalisation is essentially one of grooming by others. I will report any concerns immediately to the DSL or principal.
- I understand that as part of the disciplinary process for misconduct or where a legitimate genuine concern has been raised, my school files, e-mails and internet access history will be accessible to my line manager, the principal and/or an investigating officer.

Data

- I understand the definitions of sensitive and personal data.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not use any unencrypted devices to store sensitive or personal data.
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- When I leave a computer I will log off or otherwise lock it so content cannot be accessed by others.

Copyright and publication

- I will respect copyright and intellectual property rights.

- I understand and will abide with copyright law as described in the posters displayed in reprographics areas in school.
- I have accessed the website http://www.copyrightandschools.org/# and understand and will abide by copyright law in relation to online and electronic materials.
- I will not publish any defamatory and/or knowingly false material about the academy or the Trust, my colleagues and/or our pupils, neither will I post anything that could bring the academy or Trust into disrepute.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school. I have read and understood the Trust's ICT and e-Safety Policy. I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Signature
……

Date ……

Full Name …….. (printed)

Authorised Signature (Head teacher/Cover Manager)

Is this member of staff temporary? NO / YES If yes, contract end date: ……

I approve this email account / connection to the Internet / Intranet / Email.

Signature …….. Date ……

Full Name ……..
(printed)

Supply Staff Details

Address _____

_____

_____

_____

Post Code _____

Telephone _____

D.O.B. _____

Appendix 4

Contractor/Supplier ICT Acceptable Use Agreement
<x GAET academy> is hereinafter referred to as "the company."
The term “Contractor” is synonymous with “Supplier” and “3rd Party” in this document.

Overview

Where a contractor has access to the company network, including e-mail, internet, remote access and other information systems this agreement establishes basic principles necessary for the secure use and management of company information and information systems.
The contractor must sign this agreement in addition to the company confidentiality agreement.

Purpose

The purpose of this agreement is to protect the company information and information systems.

Scope

The agreement applies to all contractors employed or engaged by the company who have access to company information, electronic or otherwise, either on-site or from a remote location.

Agreement

Information Assets / Data Protection / Network

All company information assets (e.g. data, databases, reports, communications, manuals, documentation for systems, procedures, and plans) are considered "company confidential", unless expressly stated otherwise by the Company.
Contractors are expected to make every effort to ensure that all information is protected from inadvertent disclosure to any other party
Contractors must comply with the principles of the Data Protection Act 1998 or subsequent replacements or amendments to this Act. The Contractor will be liable for any contravention of this Act where the fault lies with the contractor.
Contractors must comply with the principle of the Computer Misuse Act 1990 or subsequent replacements or amendments to this Act. The Contractor will be liable for any contravention of this Act where the fault lies with the contractor.
The company network, including e-mail, internet, remote access and all supported systems are the property of the company and are for company business use.
Contractors may only access the network and supported systems to carry out the duties assigned to them as agreed in the actual contract between the company and the Contractor.

User Authorisation and Access

Remote access will be controlled through an access account, the granting of which will be managed by the IT manager.

Remote access to the network by a contractor will only be issued where a business need is identified and then only for the permitted purpose defined in the business case. Access will only be issued to named individuals where full contact details and, if deemed necessary by senior management, picture ID (copy to be retained by the company) is available and the individual has the necessary skills to carry out the role.
The IT manager is responsible for determining the access rights to information and systems and for granting contractors appropriate access and permissions of use.
Contractors will be provided with minimum access to perform the function requiring access. Where possible this will be limited to time of-day restrictions to limit access to only hours when such access is required. In some cases, access will only be allowed on request.
The company has the right to monitor usage and prohibit or restrict the connection at any time.

Contactor responsibilities

Contractors are responsible for safeguarding his or her usernames and password and protecting them from unauthorised use. Contractors are prohibited from disclosing or sharing username or passwords with others.
Contractors are accountable for any incident arising from improperly protected personal username and passwords. Compromised passwords and/or username must be immediately changed and the IT Manager informed.
Contractors may not use company systems to knowingly compromise other third party systems, networks, safeguards, or express views or distribute material that can harm or damage the reputation of the Company.
E-mail messages may be read by someone other than the person to whom it was sent and may have to be disclosed to outside parties or courts in connection with litigation. Accordingly, e-mail messages should be courteous, professional, and business-like.
Any unauthorised attempt to access information that is outside the Contractor's "need-to-know" for his/her permitted purpose is prohibited.
Any unauthorised attempt to discover the password of another user or to access company information or systems using another person's password or username is prohibited.
Contractors must ensure their own systems have adequate security policies in place and that all systems and devices used to carry out company business have up-to date virus protection. Evidence may be requested by the company.
Contractors are prohibited from attempting to bypass company virus protection software or other system security procedures.
Contractors must not install or use unapproved software to access company information systems for any purpose unless permission specifically granted by the IT Manager.
Personal computers, laptops, tablets, smartphones, and other devices containing company systems information must be secured by their users from theft and unauthorised use.
All information security incidents (e.g. malicious code, worms, viruses, unauthorized or inappropriate email/internet use) that may impact company systems must be immediately reported to the IT Manager upon discovery.

Loss of desktop, portable, or mobile computing devices by any means (e.g. theft, loss, breakage) that are used to access company systems must be reported to the IT Manager as soon as discovered to ensure that all access accounts are disabled.
The contractor agrees to fully indemnify and to hold the company indemnified and harmless from and against all losses, costs, actions, claims, expenses or liabilities whatsoever suffered or incurred directly or indirectly in consequence of the Contractor's breach or non-observance of this Agreement.

Agreement Compliance

Compliance Measurement

The Information security team will verify compliance to this agreement through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the agreement owner.

Exceptions

Any exception to the agreement must be approved by the Information security team in advance.

Non-Compliance

An employee found to have violated this agreement may be subject to disciplinary action, up to and including termination of employment.

Related Policies and Procedures

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Contractor Approval

I have read, understood and agree to the **Contractor/Supplier ICT Acceptable Use Agreement**

Company: _____

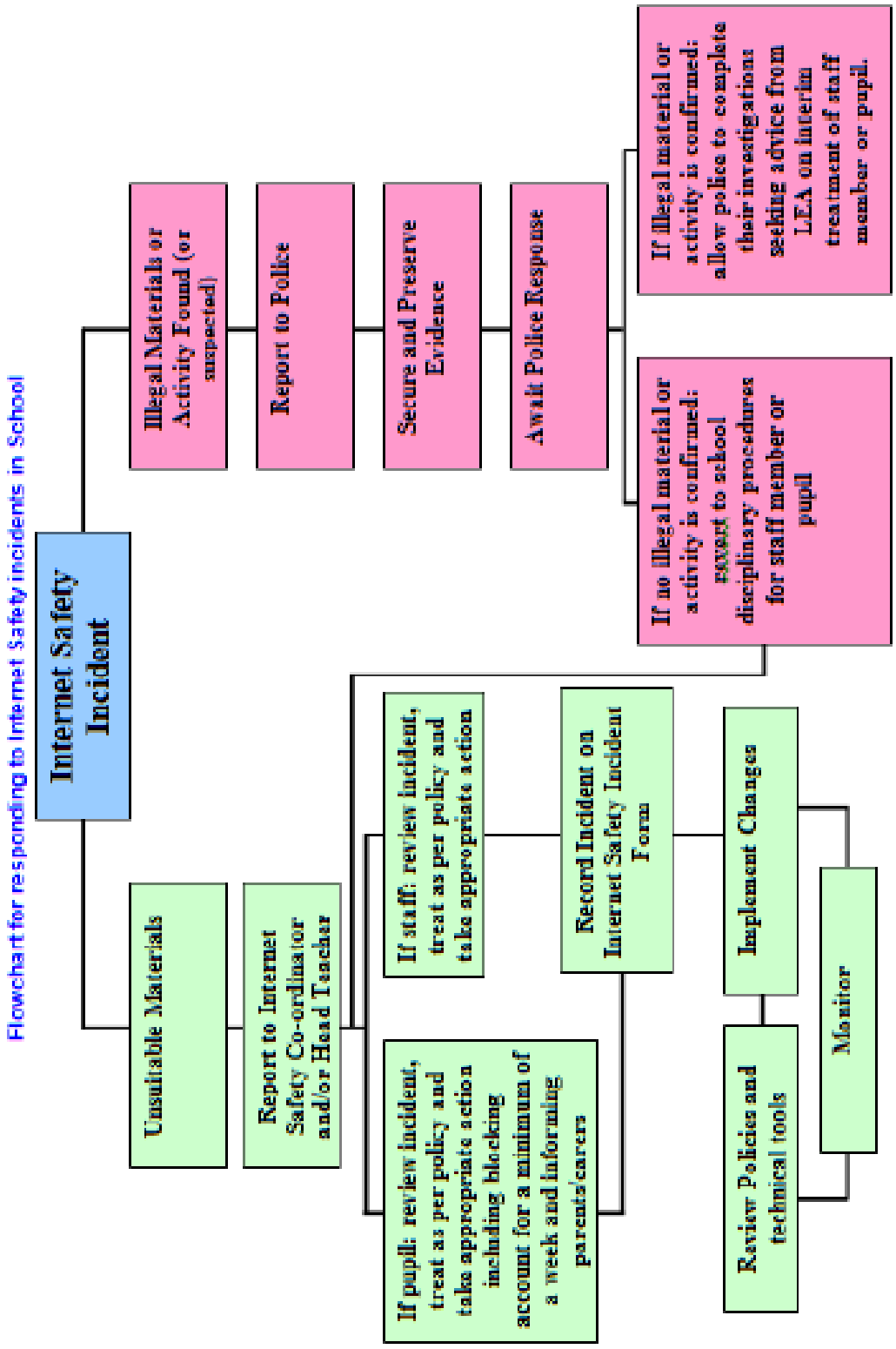
Name: _____

Position: _____

Date: _____

Signature: _____

Appendix 5
Internet safety incident



Appendix 6

School: Great Academy Ashton

ICT safety lead: Ian Phillips

Designated safeguarding lead: Rachel Gill

School's approach to pupils' own devices including mobile phones and memory sticks: Please refer to NCA Mobile Phone Policy. At NCA we discourage staff from using external storage devices as they are a data security risk and should not be needed. Exceptions may be made for visitors or new staff arriving to the academy initially uploading resources, in this case please seek advice in the first instance from Ian Phillips.

How to report intentional or unintentional access to inappropriate material: This should be reported to the Designated Safeguarding Lead, Rachel Gill.