ICT & E-safety POLICY

CONTENTS

Version: 1
Adopted: Autumn Term 2021
Next Revision Date: Autumn term 2022

1. AIMS

This policy aims to ensure that ICT makes a positive contribution to our working and learning environment within the context of awareness 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 Academies' 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.

Every GAET academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

➢ **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

➢ **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

➢ **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

➢ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for academies on:

Teaching online safety in academies

Preventing and tackling bullying and cyber-bullying: advice for Principals and academy staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. APPROPRIATE AND SAFE USE OF EQUIPMENT

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

3.1 Academy equipment

Inventory, signing out, recall of equipment, safe storage
Each GAET academy will keep centrally a full list of all ICT equipment held by the academy, 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.

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, encryption must be enforced.

Academy mobile phones
For events such as academy trips and sporting events, a academy 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 academy and agreed by the principal or Designated Safeguarding Lead (DSL).

Cameras, video cameras, webcams and related software/applications
These must be used in line with the Trust's Child Protection and Safeguarding 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 academy will be deleted if no longer needed or archived on the academy network only.
- For academy trips or visits, academy 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 academy 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 named persons, 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 academy 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 academy 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;

3.2 Protecting equipment and data

Academy network

- Academy 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 the academy has received a subject access request, because a staff member is off site and cannot get full access, because a technical difficulty is encountered requiring remote support, or if the member of staff is on sick leave. This access will only occur with the permission of the member of staff concerned or with prior notification.

- 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.
- *For safeguarding purposes, to ensure the safety of all users, the academy uses SMOOTHWALL digital safety technology to monitor academy devices. If the SMOOTHWALL technology identifies any language which may signify a potential safeguarding issue or concern in any content searched for or typed by a pupil on an academy device, then an alert is sent to the designated safeguarding lead who will follow up under the normal safeguarding procedures. Similarly, the same applies regarding staff: an alert is sent to the principal for further investigation.
- 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 academy 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 academy network.

Passwords and anti-virus/malware protection

- Passwords must be set by each user.
- Passwords should be a minimum of 7 characters and must contain letters, numbers & special Characters such as *&^%$.
- 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 academy'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 academy 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 academy and encrypted. This includes lists of pupils' names, academy 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 academy campus, another Trust academy or the Trust'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 academy 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. The disposal of ICT equipment should only be carried out by the ICT department in conjunction with the Trust ICT Manager.

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 by the Trust's ICT manager will 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.

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 academy 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.

The Trust has a contract in place with a certified disposal contractor. The disposal of all electrical equipment should be in line with the WEEE (Waste Electrical and Electronic Equipment) directive. All data baring equipment should be securely sanitised using HMG Infosec Standard 5 as a minimum. All WEEE and data destruction evidence/certificates should be retained.

On disposal, the item must be removed from the inventory and the Trust's finance assets register.

3.3 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 Academies. The individual academy appendix will say if this is so. Any use of mobile devices in academy by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy, which may result in the confiscation of their device.

If the use of a personal mobile device is allowed by the academy, 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 academy time.

4. ROLES AND RESPONSIBILITIES

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

4.1 GAET Trust Board

Ensures:

- policy implementation and review;
- monitoring of data breaches;
- support for data requests.

4.2 Trust ICT Manager

Ensures:

- an appropriate ICT strategy is in place across the Trust including a disaster recovery plan;
- ICT services and operational practices are understood across the Trust;
- appropriate levels of system controls are described in policy and understood across the Trust;
- a sound ICT service is in place in each academy within budgets;
- trust officers are advised on the ICT solutions for all statutory and regulatory responsibilities in collaboration with the Trust's Director of Governance and Compliance.

4.3 The Local Governing Committee (LGC)

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The LGC will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is [role of individual].

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3)

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.4 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

4.5 The designated safeguarding lead (DSL)

Details of the academy's DSL and deputy/deputies are set out in our safeguarding and child protection policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in academy, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the Principal and/or local governing committee (LGC).

4.6 The academy's ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at academy, including terrorist and extremist material
- Ensuring that the academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the academy's ICT systems on a [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy.

4.7 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Participating in training
- Supporting and contributing to a curriculum approach to safety, including issues of personal safety, self-esteem, bullying – including cyber bullying and prejudice-based bullying, relationships, sex and health education, domestic abuse, child sexual or criminal exploitation, radicalisation, honour-based violence and forced marriage
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3), and ensuring that pupils follow the academy's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

4.8 Parents/carers

Parents and carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

4.9 Visitors and members of the community

Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

5. EDUCATING PUPILS ABOUT DIGITAL WELLBEING AND ONLINE SAFETY

The world of online learning and virtual environments and the intellectual stimulation it provides can help pupils feel more connected to others, more productive and more engaged. However, learning and delivering services online can also make pupils feel disconnected and fatigued, as well as increasing their concerns about staying motivated and absorbing the material. This may lead to pupils feeling lethargic and drained, and can contribute to spikes in anxiety and low mood. Therefore, pupils need to understand the need for adopting a healthy balance between onscreen and offscreen activities and lifestyle.

Pupils will be taught about digital wellbeing and online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All academies have to teach:

Relationships education and health education in primary academies

Relationships and sex education and health education in secondary academies

Primary academies insert:

In **Key Stage 1**, pupils will be taught to:

- ✓ Use technology safely and respectfully, keeping personal information private;
- ✓ Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- ✓ Use technology safely, respectfully and responsibly;
- ✓ Recognise acceptable and unacceptable behaviour;
- ✓ Identify a range of ways to report concerns about content and contact.

By the **end of primary school age**, pupils will know:

- ✓ That people sometimes behave differently online, including by pretending to be someone they are not;

- ✓ That the same principles apply to online relationships as to face-to-face; relationships, including the importance of respect for others online including when we are anonymous;
- ✓ The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- ✓ How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- ✓ How information and data is shared and used online;
- ✓ What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
- ✓ How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Secondary academies insert:

In **Key Stage 3**, pupils will be taught to:

- ✓ Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- ✓ Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- ✓ To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- ✓ How to report a range of concerns.

By the **end of secondary school age**, pupils will know:

- ✓ Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- ✓ About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- ✓ Not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- ✓ What to do and where to get support to report material or manage issues online;
- ✓ The impact of viewing harmful content;
- ✓ That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- ✓ That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail;
- ✓ How information and data is generated, collected, shared and used online;
- ✓ How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;

- ✓ How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. EDUCATION PARENTS ABOUT DIGITAL WELLBEING AND ONLINE SAFETY

The academy will raise parents' awareness of digital wellbeing and internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Digital wellbeing and online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL. In relation to digital wellbeing parents should contact the academy's mental health lead and/or the relevant pastoral year team.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

7. CYBER-BULLYING

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy's behaviour policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form tutors will discuss cyber-bullying with their classes and tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of academy discipline), and/or
- Report it to the police*.

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- ➢ The DfE's latest guidance on screening, searching and confiscation
- ➢ UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- ➢ The academy's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the academy complaints procedure.

8. ACCEPTABLE USE OF THE INTERNET WITHIN THE ACADEMY

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

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.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. 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 academy 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 academy staff, for example the designated safeguarding lead, e-Safety Co-ordinators or the Network Manager.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Considerate use of the internet and email

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 academy, 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.

Whenever e-mail is sent using your academy account, the sender's name, job title, e-mail address and the academy'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 academy that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the academy's guidelines).
- You should be aware that, in the event of the academy 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 a personal device will need to ensure that the 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.
- As a general rule, full names of staff or pupils should not be used within the subject line or body of an email. Initials should be used where possible.

9. STAFF USING WORK DEVICES OUTSIDE THE ACADEMY

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

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

- Use social media with care. The use of the maximum security and/or privacy settings available is strongly recommended. Seek advice if you require assistance in setting up security settings. Academy staff should be aware of the requirement to uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside academy.
- 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 academy. Best practice guidance is that students must have left the academy 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' – you should notify the DSL if this is the case.
- If there are exceptional circumstances, e.g. you have a relative at the academy who is linked to you on social media, you must follow the academy'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.

10. REMOTE LEARNING

The GAET ICT manager will ensure that the academy is using a platform that is suitable for the children's age group, stage of development and ability. Academy accounts will be set up for any online platforms that are used (teachers' personal accounts must NOT be used). Staff will double check their privacy settings.

Teaching online is different to teaching face-to-face. Staff should always maintain professional relationships with children and young people. The academy will remind staff of the code of conduct and make it clear how they are expected to behave.

If recording or live streaming lessons, teachers must ensure that they are in a neutral area where nothing personal or inappropriate can be seen or heard in the background. They must also make sure that children are in a neutral area if they can be seen on camera.

It is best practice to have at least two adults present when working with pupils. This applies both on- and offline. The number of adults needed for online lessons will vary depending on the children's age and stage of development, and the activities being carried out. If 'breakout rooms' are being used on an online platform, these will need to be supervised. The academy will ensure that staff are trained in all aspects of remote learning safety.

Sometimes staff might need to contact pupils individually, for example to give feedback on homework. This should be done using MS Teams which is monitored by the academy. Academy staff should only contact children during normal academy hours, or at times agreed by the academy leadership team (DfE, 2021). Any one-to-one sessions, for example pastoral care meetings, should be risk assessed and approved by the academy's leadership team (DfE, 2021).

Staff will receive training so that they know what safeguarding measures to take if they are having a one-to-one conversation with a pupil, and what to do if they have any concerns about a pupil's welfare.

10.1 How pupils report concerns during remote learning

Pupils will be informed to contact the DSL if they need to report a concern whilst on remote learning. Pupils will all have access to the DSL via MS TEAMS. Additionally, pupils will be made aware of other national organisations that they can contact if they would prefer, eg. NSPCC helpline, Childnet etc.

11. HOW THE ACADEMY WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the academy's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. These are recorded initially using the academy's online safeguarding system and then on the online safety incident report log (Appendix 5) once investigated and confirmed.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the LGC. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. LINKS TO OTHER POLICIES

This online safety policy is linked to our:

Safeguarding and child protection policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Adapt this agreement to reflect your academy's approach, in line with any changes you made to this policy

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in the academy I will:

Ask a teacher or adult if I can do so before using them

Only use websites that a teacher or adult has told me or allowed me to use

Tell my teacher immediately if:

- I click on a website by mistake
- I receive messages from people I don't know
- I find anything that may upset or harm me or my friends

Use school computers for school work only

Be kind to others and not upset or be rude to them

Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

Only use the username and password I have been given

Try my hardest to remember my username and password

Never share my password with anyone, including my friends.

Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

Save my work on the academy network

Check with my teacher before I print anything

Log off or shut down a computer when I have finished using it

I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil): **Date:**

Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer): **Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

Adapt this agreement to reflect your academy's approach, in line with any changes you made to this policy

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the academy's ICT systems (like computers) and get onto the internet in school I will:

- Always use the academy's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the academy's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into the academy:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in the academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Adapt this agreement to reflect your academy's approach, in line with any changes you make to this policy.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
• **When using the academy's ICT systems and accessing the internet in the academy, or outside the academy on a work device (if applicable), I will not:** • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the academy's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network • Share my password with others or log in to the academy's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the academy, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the academy	
I will only use the academy's ICT systems and access the internet in the academy, or outside the academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

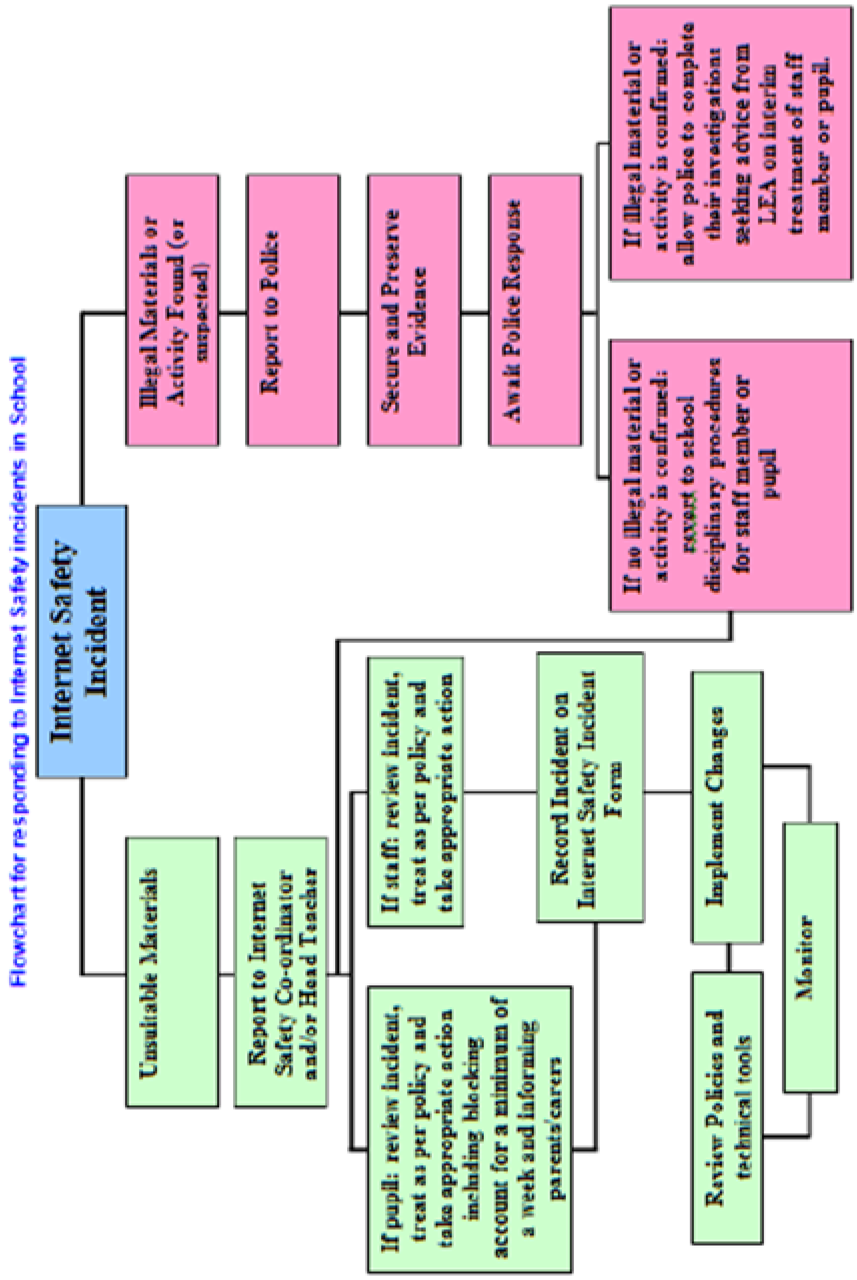
Adapt this form to suit your needs

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in the academy?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 6: internet safety incident flowchart


Flowchart for responding to Internet Safety incidents in School
Internet Safety Incident
Illegal Materials or Activity Found (or suspected)
Report to Police
Secure and Preserve Evidence
Await Police Response
If no illegal material or activity is confirmed: revert to school disciplinary procedures for staff member or pupil
If illegal material or activity is confirmed: allow police to complete their investigation; seeking advice from LEA on interim treatment of staff member or pupil.
Unsuitable Materials
Report to Internet Safety Co-ordinator and/or Head Teacher
If staff: review incident, treat as per policy and take appropriate action
If pupil: review incident, treat as per policy and take appropriate action including blocking account for a minimum of a week and informing parents/carers
Record Incident on Internet Safety Incident Form
Implement Changes
Review Policies and technical tools
Monitor