Online Safety and Acceptable use Policy

Contents

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of students, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 Department’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 students' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing body

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

The governing body 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 Katie Tarrant (Safeguarding Governor)

Chair of Governors: Dee Wilson

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)

3.2 The Principal

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

Principal: Matt Robertson

3.3 The Designated Safeguarding Lead

Details of the Academy's DSL [and deputies] are set out in our child protection and safeguarding policy as well relevant job descriptions.

DSL: Steve Taylor
Deputy DSLs: Steph Garrad, Pauline McLeod

The DSL takes lead responsibility for online safety in the 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 network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 3) 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 governing body

This list is not intended to be exhaustive.

3.4 The ICT network manager

The ICT network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students 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** 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 4) 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

This list is not intended to be exhaustive.

3.5 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
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2), and ensuring that students follow the Academy's terms on acceptable use (appendix 1)
- 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

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/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 (appendix 1)

Parents/carers 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/carer factsheet - Childnet International

3.7 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 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

From September 2020 the Academy will deliver: Relationships and sex education and health education as part of its statutory obligation. (Statutory from Summer term 2021)

This new statutory requirement includes aspects about online safety. As such we have added these expectations in italics below,

In **Key Stage 3**, students 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

Students 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 Key Stage 4** students 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 these behaviours

In addition, The Academy will:

Promote the safe use of social media and the internet in other subjects where relevant.

Use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents/carers about online safety

The Academy will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. All parents/carers also have access to **The National Online Safety programme (NoS)**. Parents/carers have access to their own account and can access appropriate resources, and materials. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings/forums.

If parents/carers 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.

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

6. Cyber-bullying

6.1 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 anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

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

The Academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed through assemblies, PSHE/RSE and Inspire days.

Teaching staff are 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 students, as part of safeguarding training.

The Academy also sends information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected. Information is also available through the NoS programme.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy/anti-bullying policy. Where illegal, inappropriate, or harmful material has been spread among students, 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, including the Academy's School Early Intervention Officer (SEIO)

6.3 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 students' 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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. And the Academy behaviour policy

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

7. Acceptable use of the internet in the Academy

All students, 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.

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.

We will monitor the websites visited by students, 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.

8. Students and mobile device use

Students may bring mobile devices into the Academy, but they are not permitted to use them at all during the Academy day. All devices must be switched off on entry to site and should not be seen or heard at all. Devices may be used again on departure from site, but not until being off the Academy campus.

Any student whose mobile device is seen or heard, will have it confiscated and returned at the end of the Academy day. If this is repeated, a parent will have to collect the device and speak to a member of the SLT

Any breach of the Acceptable use agreement by a student may trigger disciplinary action in line with the Academy behaviour policy, which may result sanctions, including exclusion.

9. Staff using work devices outside the Academy

Staff members using a work device outside Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside Academy. Any USB devices containing data relating to the Academy **must be encrypted**.

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

Work devices must be used solely for work activities.

10. How the Academy will respond to issues of misuse

Where a student 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/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).

The DSL and 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 about 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. Remote learning

The Global pandemic (Coronavirus) in 2020 necessitated a growth in remote and online learning as students were unable to attend normal Academy provision. This enabled the Academy to deliver and support learning in new and innovative ways. The following guidelines should be adhered to when setting and facilitating online and remote learning to ensure students' safety and welfare.

- Staff should only use approved platforms/applications to set/deliver online learning, including Show My Homework, Class-charts, Microsoft Teams, and Google Classrooms, as part of a coordinated approach
- Staff should only communicate with students via these platforms and the use of approved Academy email addresses
- Sessions should be properly scheduled, and attendance recorded
- Where webcams are used, staff should always have their camera turned off, so that students cannot see them or their surroundings. I some cases, when delivering content student microphones should be muted, but can be unmuted for questions
- Staff should report any safeguarding concerns that may arise during online learning session through the normal channels and inform the DSL

13. Monitoring arrangements

The DSL/safeguarding team log behaviour and safeguarding issues related to online safety on CPOMS (Child Protection Online Monitoring and Safeguarding). An incident report log is also used, a copy of which can be found in appendix 4.

This policy will be reviewed annually by the **Designated Safeguarding Lead**. At every review, the policy will be shared with the governing body.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers)

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

Name of student:

I will read and follow the rules in the acceptable use agreement policy
This acceptable use document is intended to ensure:

- our students show respect for Academy ICT equipment and use it responsibly and show respect for others in their online activities, both in and out of the Academy.
- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that the Academy's ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The Academy will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

I understand that I must use the Academy's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email, and other digital communications
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password, nor attempt to access other people's accounts
- I will be aware of "stranger danger", when I am communicating on-line and not put my personal safety at risk by engaging in communication with people that I do not know.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a responsible adult (parent, teacher etc).

I will stick by the **SMART** rules on being online (**S**afe- don't give personal details, **M**eet-never arrange to meet anyone I have met online, face to face without an adult being present, **A**ccept-not accept unfamiliar messages and email attachments from unknown sources- I will report these, **R**eliable-I will remember that not everything online is true/accurate a lot of content is inaccurate or opinion, **T**ell- I will tell a responsible adult if I am worried about any unpleasant/worrying online behaviours.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will only use IT systems when a teacher/member of staff is present, or with a teacher's/member of staff's permission.
- I will not attempt (unless I have permission) to make downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions. I will always 'click with compassion'.
- I will not take or distribute images (still images or video) of anyone without their permission/consent. This is not permitted under the Data Protection Act 2018/GDPR.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the Academy's day to day effective operation:

- I will not use my personal mobile phone or other electronic devices in the Academy, in line with policy, and to avoid disruption to learning.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others when using Academy I.T. equipment, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving hardware or software; however, this may have happened.
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing malware.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites which are not permitted.
- I will always log off or shut down a computer when I am finished working on it.

When using the internet for learning, research, or other purposes, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work. I will also reference sources properly is using them to support my studies.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that as a member of the Arnold Hill Community, I am responsible for my actions, **both in and out** of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (**examples would be cyber-bullying, inappropriate use of images, personal information and/or inappropriate use of social media, particularly where it adversely affects others or brings the Academy into disrepute**).
- I understand that if I fail to comply with this Acceptable Use Agreement, I may be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, exclusions, contact with parents and in the event of illegal activities, involvement of the police/other external partners.

Please complete the section below to show that you have read, understood, and agree to the requirements of the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to Academy's ICT systems/equipment.

Students should be aware that misuse of ICT equipment or inappropriate online behaviour may be against UK Law and be subject to investigation/action covered in this legislation:
Malicious Communication Act 1988
Computer Misuse Act 1990
Communications Act 2003
Equality Act 2010
Serious Crime Act 2015

Student Acceptable Use Agreement Declaration:
This form relates to the student Acceptable Use Agreement to which it is attached.
Please complete the sections below to show that you have read, understood, and agree to the requirements included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to the Academy's ICT systems/equipment.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy's ICT systems and equipment (both in and out of the Academy)
- I use my own equipment outside of the School in a way that is related to me being a member of this Academy e.g. communicating with other members of the School, accessing email, VLE, website etc.

I also agree to ensuring that my online activities will always show due respect for others, not cause offence, or bring the reputation of the Academy into disrepute.

Signed (student):	**Date:**

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 students using the Academy's ICT systems, use of technology and the internet and will make sure my child understands these.

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

Appendix 2: Acceptable use agreement (staff, governors, volunteers, and visitors)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. Additionally, that I am expected to demonstrate respect for ICT equipment provided by the Academy and respect for others in my online activities and behaviours.

I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

General:

- I agree to take care of all Academy ICT equipment issued to me for my professional use including Laptops. Desktops and any other equipment issued to me to support my professional duties.
- If I choose to take portable equipment home with me, I will transport it carefully and ensure it is kept secure offsite to avoid damage or risk of data breach.
- If I chose to leave portable equipment issued to me at The Academy overnight/over a weekend/holiday I will ensure it is securely locked away.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the ICT systems, e-mail, and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Academy ICT systems (e.g. laptops, email, remote connection, social media etc.) out of the Academy.
- I understand that the Academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Academy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- When logged on to an Academy device, if I leave the device for any reason, I will lock it so it cannot be accessed by an unauthorised user (Windows 'L').
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, to the appropriate person (DSL or Principal).
- I will ensure that I maintain high levels of security by using secure passwords and updating these when requested; I will also act upon any Trust/Academy advice to maintain network and IT systems security including use of email.
- I will ensure Academy devices are regularly connected to the Academy network so that relevant software/hardware updates are made, and security is not compromised.
- I will not allow any persons, other than approved Academy staff to use equipment provided to me in my role within the Academy.

I will be professional in my communications and actions when using Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission, or permission of a line manager in the event of illness etc.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions, in line with the Academy's email code of conduct.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital / video images and the code of conduct. I

will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the Academy website / Social Media etc.) it will not be possible to identify by name, or other personal information, those who are featured.

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only engage in email conversations with students/parents/carers by using my Academy email. I will not use any personal email services for this purpose.

Electronic Mail:

I have been provided with email facilities and will use them responsibly:

- Caution should be exercised when sending confidential information via e-mail.
- Student names should not be used in the subject line of any emails, only initials. Emails containing sensitive information should be encrypted.
- The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited.
- You may make reasonable use of Academy facilities for personal e-mails, if this does not have more than a minimal impact on resources and does not adversely affect your work or the work of others.
- While the Academy respects the privacy of staff, where there is reason for concern, the Academy reserves the right to monitor and intercept e-mail communication.
- Any e-mail communication made must not bring the Academy into disrepute; this includes anything libellous, defamatory, or criminal.
- All external emails, both inbound and outbound are filtered for content. This includes obscene language and suspect attachments that could contain malware.
- Staff should be aware that content of emails may be requested for disclosure in a SARs (Subject Access requests) under the Data Protection Act 2018, or as a freedom of information (FOI) request.

The Academy and Spencer Academy Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of IT systems. I agree:

- When I use my personal hand-held / external devices (PDAs / laptops / mobile phones / smartwatch/ USB devices etc.) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date security software and are free from malware.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing malware or other harmful programmes. I will report any suspicious emails to the I.T. network Manager.
- I will not access websites which, if seen by students could cause embarrassment to myself or others (dating websites etc.).
- I will ensure that my personal data on my laptop is backed up as I am aware that data stored outside of ‘Networked drives’ is not automatically backed up by Academy systems.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- •I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their professional duties.
- I will not install or attempt to install programmes / Software that is not related to my role within the Academy. I will always consult the Network Manager prior to purchasing software to hardware to check compatibility/security issues.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others. If I accidentally damage Academy I.C.T. equipment, I will report this to line management and/or I.C.T. support staff.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened (IT helpdesk)

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Data Protection Policy. Where Student/sensitive data is transferred outside the secure Academy network, it must only be with Agreed third party suppliers who comply with GDPR/DPA 2018 and must also be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos) without the owner's consent

I understand that I am responsible for my actions in and out of the Academy:

- I understand that this Acceptable Use Document applies not only to my work and use of the Academy's ICT equipment in the Academy, but also applies to my use of Academy ICT systems and equipment out of the Academy and my use of personal equipment in the Academy or in situations related to my employment by the Academy.
- I understand that if I fail to comply with this Acceptable Use Document Agreement, I could be subject to disciplinary action.
- Staff should be cautious when using social networking sites outside of work and avoid publishing, or allowing to be published, any material, including comments or images, that could damage their professional reputation and/or bring the Academy into disrepute. Staff should be strongly advised to set their profile as 'private' and to ensure privacy settings reflect maximum levels of security, thus not allowing access to students, their families and/or carers. Locally, there have been incidents of students misinterpreting the nature of their relationship with members of staff as a direct result of them having contact on social networking sites.
- Staff should also be mindful that requirements in relation to maintaining the confidentiality of students, their families, colleagues, and the Academy itself apply to all forms of communication, including that which takes place on social networking sites.

I have read and understand the above and agree to use the Academy ICT systems (both in and out of the Academy) and my own devices (in the Academy and when carrying out communications related to the Academy) within these guidelines.

I understand that misuse of ICT equipment and or inappropriate online behaviour may contravene the Staff Code of Conduct and may constitute an offence under UK Law (as in legislation below):

Malicious Communication Act 1988
Computer Misuse Act 1990
Communications Act 2003
Equality Act 2010
Serious Crime Act 2015

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 student 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 students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

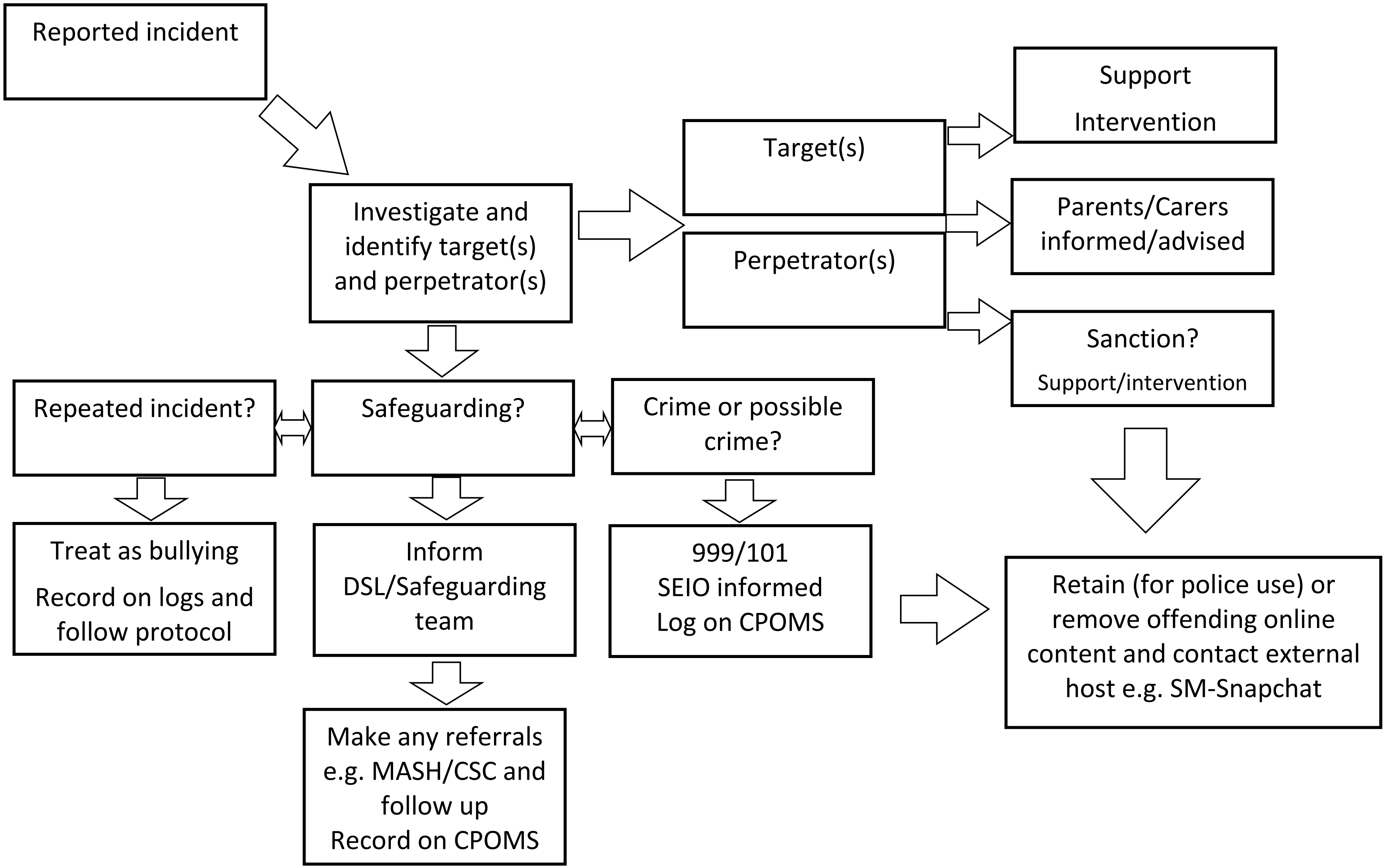
Appendix 3: Online safety training needs – self audit for staff

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?	
Do you know what you must do if a student 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 students 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 4: 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 5: Online safety/incident/cyberbullying- Actions flow chart



Reported incident
Investigate and identify target(s) and perpetrator(s)
Target(s)
Perpetrator(s)
Support
Intervention
Parents/Carers informed/advised
Sanction?
Support/intervention
Repeated incident?
Safeguarding?
Crime or possible crime?
Treat as bullying
Record on logs and follow protocol
Inform DSL/Safeguarding team
999/101
SEIO informed
Log on CPOMS
Retain (for police use) or remove offending online content and contact external host e.g. SM-Snapchat
Make any referrals e.g. MASH/CSC and follow up
Record on CPOMS