



Online Safety Policy

Author	Kirstie Moore, Assistant Headteacher
Date	October 2021
Date for review	October 2022

Contents

1. Introduction and Aims	3
2. Legislation and guidance.....	4
3. Roles and responsibilities.....	4
4. Educating students about online safety	7
5. Educating parents/carers about online safety.....	7
6. Cyber-bullying	8
7. Acceptable use of IT at Alde Valley Academy	9
8. Use of mobile devices in school	12
9. Staff using work devices outside school	12
10. Social Media - Protecting Professional Identity.....	13
11. How the academy will respond to issues of misuse	13
12. Training	144
13. Filtering and Monitoring arrangements	155
14. Links with other policies	166
Appendix 1: Acceptable use agreement (pupils and parents/carers) Error! Bookmark not defined.	7
Appendix 2: Acceptable use agreement (staff, committee members, volunteers and visitors). Error! Bookmark not defined.	8
Appendix 3: Computer Science Online Safety curriculum.....	19

1. Introduction and Aims

This policy applies to all members of the Alde Valley Academy community (including staff, students, parents/carers and any visitors) who have access to and are users of the Academy's ICT systems, both in and out of the school. With the continued increase in use of technology and the internet, it is the duty of Alde Valley Academy to ensure that young people are protected from potential harm both within and beyond our school setting, whilst effectively using these resources to have the best possible education, and connections with people which are safe.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

This policy aims to explain how everyone can be a part of these safeguarding procedures. It also details how students are educated to be safe and responsible users, capable of making good judgements about what they see, find and use. Online safety refers to the act of staying safe online. It is also commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets.

<https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety>

Alde Valley Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Academy Committee members, which includes providing safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- 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 schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school 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.

3. Roles and responsibilities

3.1 The Trust and Academy Committee

The Waveney Valley Academies Trust Board has a legal responsibility to make sure that there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children and young people's welfare, and to monitor that the school complies with them, holding the headteacher to account for its implementation.

Through the Scheme of Delegation, the Trust Board delegates the responsibility for monitoring school safeguarding matters to the Academy Committee who ensure that the Academy's students are safeguarded from potentially harmful and inappropriate online material. The Academy Committee should ensure that the policy is made available to parents and carers by publishing this on the school website or in writing if requested.

All Academy Committee members 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 2)
- 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

3.2 The headteacher

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

As with behaviours offline, the headteacher will follow guidelines set out in the academy's safeguarding and child protection policy in relation to allegations against members of staff online.

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher, ICT systems 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 school safeguarding child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this and policy, as well as the safeguarding and child protection policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policy
- Review the online safety/bullying logs to inform the future of any online safety developments
- Updating and delivering staff training and updates on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online bullying/safety in school to the headteacher and/or Academy Committee Trust

This list is not intended to be exhaustive.

3.4 The ICT systems manager

The ICT manager is responsible for:

- Ensuring the academy meets required online safety technical requirements and any MAT Online Safety Policy / Guidance that may apply
- 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 school or using school online platforms, 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 to ensure the academy's technical infrastructure is secured as much as possible and is not open to misuse or malicious attack
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Keeping up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

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 school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Ensuring that students are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. They should know what to do in the event of an incident.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and anti-bullying 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'
- Using electronic communications in an appropriate way that does not breach the Data Protection Act 2018. Remember confidentiality and to not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Reporting accidental access to inappropriate materials to the DSL/Online Safety Lead in order that inappropriate sites are blocked where possible.
- Ensuring that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school'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 resource sheet – [Childnet International](#)

Healthy relationships – [Disrespect Nobody](#)

Online Safety Advice - <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

3.7 Visitors and members of the community

Visitors and members of the community who use the school'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. The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app (Teaching Online Safety in Schools, DFE, 2019).

At Alde Valley Academy we teach Online Safety within our Computer Science curriculum (see appendix 3), PSHE lessons, personal development sessions in tutor time and also have dedicated assemblies which link to a whole school half termly theme. We aim to educate our students so that they understand the risks and can make sensible and informed choices online; allowing them to make most of the internet and devices, staying safe whilst doing so.

During a variety of sessions across the curriculum students will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

The Computer Science curriculum and [Relationships and sex education and health education](#) in secondary schools has been used when planning Personal Development sessions to ensure the programme enhances students' learning further.

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 students with SEND.

5. Educating parents/carers about online safety

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will raise parents'/carers' awareness of online safety in letters or other communications home, and in information via our website or social media accounts. This policy will also be shared with parents/carers and where appropriate, parent/carer sessions will be held.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or Learning Support Manager.

Concerns or queries about this policy can be raised with the Designated Safeguarding Lead or the headteacher.

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's anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will 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 victim.

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. The majority of this will take place during tutor time, Computer Science and PSHE lessons, but these sessions will not be isolated and teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying where appropriate.

All staff, committee members 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/carers 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 school behaviour and discipline policy and the anti-bullying 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.

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 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 school rules

As with all safeguarding issues, online concerns must be reported via CPOMS to the DSL.

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

- Delete that material, or
- Retain it as evidence (if a criminal offence or a breach of school discipline has taken place), 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.

All staff must be aware that if they become aware of an incident which involves the sharing of nudes they must:

- **Never** view, copy, print, share, store or save the imagery themselves, or ask a child to share or download – **this is illegal**
- If you staff already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL and seek support
- **Not** delete the imagery or ask the young person to delete it
- **Not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent)
- **Not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers
- **Not** say or do anything to blame or shame any young people involved
- Explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

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](#)

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

7. Acceptable IT use at Alde Valley Academy

All students, parents, staff, volunteers and committee members are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school'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, committee members and visitors (where relevant) to ensure they comply with the above.

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

7.1 E-mail Use

Alde Valley Academy has e-mail addresses for students and staff to use for communication purposes. This supports students in being able to understand different ways of communicating and using ICT to share and present information in different forms. Staff and students should use their school issued email addresses for any communication between home and the Academy.

Individual email accounts are monitored and can be traced if there is an incident of misuse. All E-mails which are sent and received are scanned against an objectionable word list. If any objectionable words are found the recipient and DSL are made aware so the recipient is warned of possible unpleasant content and necessary, appropriate action can be taken.

Further information regarding the academy's processes to safeguard our students online can be found in section 10.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with young people is to communicate about who they may be talking to and assess risks together.

7.2 Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. In line with the staff code of conduct, the academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites,

nor should parents/carers comment on any activities involving other students in the digital / video images. School reserve the right to ask that no filming or photography is undertaken where students are involved in group performances

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on the Academy's website or blog in association with photographs. It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications.

7.3 Video-Conferencing and Webcams

If staff are engaging in online learning with students via video-conferencing, this should not be on a 1:1 basis. There must be more than one student or member of staff present. The Academy's online platform must be used and staff should ensure the following:

- Students are invited to the lesson using their school email address
- Students cannot enter the live lesson without the member of staff admitting them
- Unknown email addresses outside of the Academy are not permitted entry
- Any students not conforming to the Academy's expectations are removed and the Student Discipline and Behaviour policy is followed
- All students are removed from the session before it is ended. This ensures students are not left on the call without a member of staff.

Where students (or adults) may be using a webcam in a family area at home, staff are encouraged to adapt their background so any personal information cannot be seen.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable User Agreement).

8. Using mobile devices in school

Students

As per the academy's discipline and behaviour policy:

No electronic gadgetry of any kind, including mobile phones should be in view in lessons or in corridors. With some students commuting to school, we understand that some parents/carers may wish for their child to have a phone with them. If students wish to bring mobile phones or other devices into school, these must be switched off and out of sight (in their bag). Alternatively, these can be handed in to the front office at the start of the day to be collected at the end of the school day. The Academy is not responsible for any theft, loss or damage of any personal mobile device.

Under no circumstances should any electronic equipment be used to take pictures of or record any individual, student or staff member, without the expressed permission of that individual. The academy reserves the right to discipline any individual where this has occurred.

Staff

Staff should be allowed to bring in personal mobile phones or devices for their own use, or may use these for some school business. Staff should not use personal email accounts in professional communications and should ensure the schools 3CX system is used for phone calls made in relation to school. Under no circumstances are staff are allowed to use personal numbers to contact children and young people, or use personal devices to take photographs/videos of Alde Valley Academy students.

- Staff must ensure that there is no inappropriate or illegal content stored on the device
- Staff should refrain from using mobile devices in the presence of students
- The Academy is not responsible for any theft, loss or damage of any personal mobile device.

9. Staff using work devices outside school

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 passwords are not shared with other individuals
- 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

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2. 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 Alde Valley Academy's IT Systems Manager.

10. Social Media – Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for students and staff. They could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Academy staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When an official school social media accounts are established these should be monitored and overseen by a member of the senior leadership team.

Personal Use:

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.

11. How the academy will respond to issues of misuse

Students

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our Discipline and Student Behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. The student may be prevented from using the Academy's IT system for a period of time.

If a student **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action.

Staff

Where a staff member misuses the school'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 code of conduct and the safeguarding and child protection policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Any member of staff who has concerns about the activity of an adult on the academy's IT system should report this to the Headteacher as per the safeguarding and child protection policy.

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. This is incorporated within the safeguarding training.

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
- The Academy has a zero tolerance to peer on peer abuse and all staff need to challenge unacceptable behaviours
- Online concerns should be reported to the DSL via CPOMS

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 team 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.

Academy Committee Members 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. Filtering and Monitoring arrangements

The academy will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. As an academy we will do all we reasonably can to limit children's exposure to safeguarding risks online. To ensure this there are appropriate filtering and monitoring systems in place.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT Systems Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for the school ICT systems, used by the ICT Systems Manager (or other person in the It team) is available to a member of senior leadership and kept in a secure place on the network.
- The ICT Systems Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Changes to filtering and monitoring are recorded by the ICT Systems Manager and any requests may be considered by ICT Systems manager with reference to Designated Safeguarding Lead and Online Safety Lead
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- *An appropriate system is in place* via helpdesk or safeguarding referral for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed AUP is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.

Online Incident monitoring

The DSL logs behaviour and safeguarding issues related to online safety. Individual incidents will be addressed as well as emerging patterns amongst student groups/whole school.

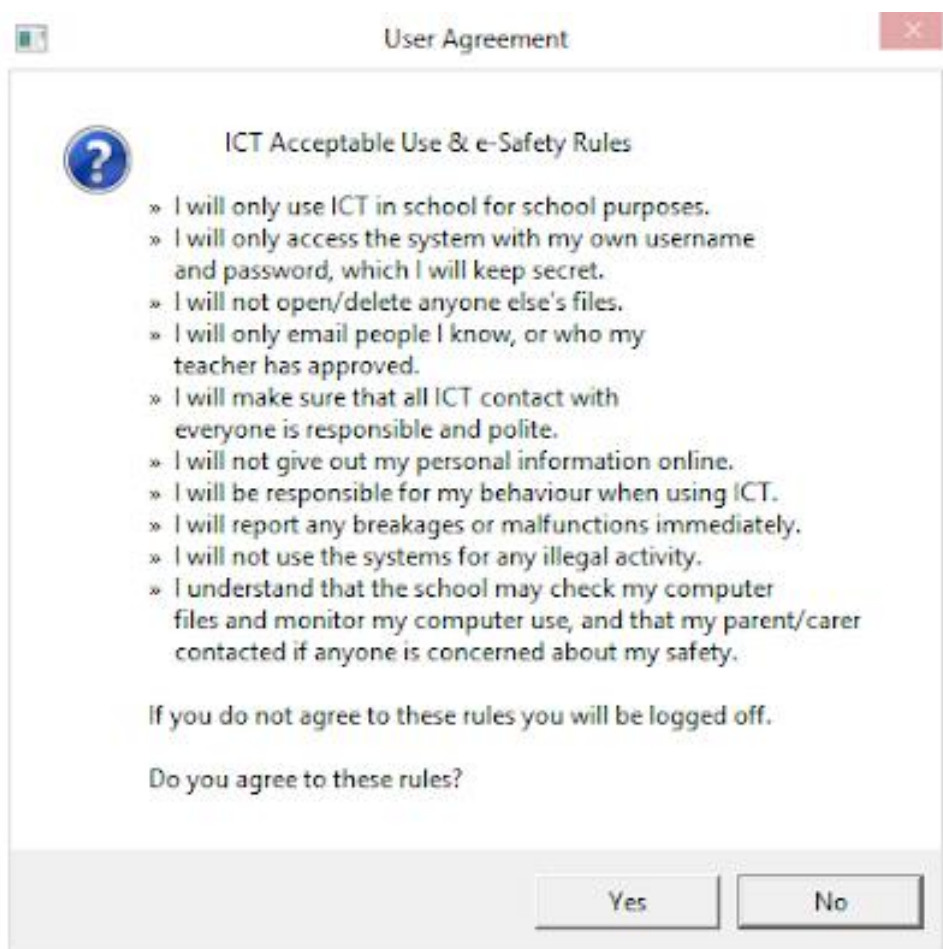
This policy will be reviewed every year by the DSL/Online Safety Lead. At every review, the policy will be shared with the Academy Trust. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Student Discipline and Behaviour policy
- Relationships and Sex Education policy
- Anti-Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable computer use policy

Appendix 1 – Student Acceptable Use Agreement

A screenshot of a 'User Agreement' dialog box. The title bar says 'User Agreement' with a close button. Inside, there is a blue question mark icon. The text reads: 'ICT Acceptable Use & e-Safety Rules'. Below this is a list of 11 rules, each preceded by a right-pointing arrow. The rules cover school use of ICT, login credentials, file management, email use, online behavior, reporting issues, and school monitoring. At the bottom, it asks 'Do you agree to these rules?' and provides 'Yes' and 'No' buttons.

User Agreement

?

ICT Acceptable Use & e-Safety Rules

- » I will only use ICT in school for school purposes.
- » I will only access the system with my own username and password, which I will keep secret.
- » I will not open/delete anyone else's files.
- » I will only email people I know, or who my teacher has approved.
- » I will make sure that all ICT contact with everyone is responsible and polite.
- » I will not give out my personal information online.
- » I will be responsible for my behaviour when using ICT.
- » I will report any breakages or malfunctions immediately.
- » I will not use the systems for any illegal activity.
- » I understand that the school may check my computer files and monitor my computer use, and that my parent/carer contacted if anyone is concerned about my safety.

If you do not agree to these rules you will be logged off.

Do you agree to these rules?

Yes No

Appendix 2 – Staff Acceptable Use Agreement

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on academy computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work, and the work of others, at risk.
- Only use the computers for educational purposes. Activities such as buying or selling goods for personal purposes are inappropriate.
- Always check files brought in on removable media with antivirus software and only use them if they are found to be clean of viruses. If you are not sure how to do this, seek advice from a member of IT Support.
- Always check mobile equipment (e.g. laptops, phones, tablet PCs, etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Don't allow anyone- even a colleague- to use your computer when you are logged on: their actions will be recorded as yours.
- Be mindful of what other computer users, including parents and students, can see of your life outside school.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you, your work, or the work of others at risk.
- The school monitors use of computer systems in school for staff and students for appropriate use, and uses a reputation checking tool to monitor internet references to the school. Even material which is immediately deleted may be picked up by our monitoring system.
- Be mindful of your 'digital footprint' and set privacy settings as high as possible on social media.
- Respect confidentiality. Lock your computer when you leave it unattended.

Internet

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the academy, as well as students or staff. This includes abiding by copyright laws.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour in email or other documents must be avoided.
- Be wary of unsolicited attachments, even from people you know. Save and scan any attachments before opening them. Attachments can contain viruses or other programs that could destroy all the files and software on your computer, including other computers on the academy network.
- If you receive an email or other electronic communication containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to online safety lead. The sending or receiving of an email containing content likely to be unsuitable for academies is strictly forbidden.

Appendix 3 – Computer Science Curriculum

Year 7 Online safety

- Understand how cyberbullying can make a person feel
- Understand the mediums by which cyberbullying can occur
- Discuss sexting - what it is and how it can be avoided
- Outline the steps to take if you every are a victim of cyberbullying or sexting (including who to speak to in school (DSLs))
- Identify measures to stay safe online
- Create an informational film showing a good understanding of staying safe online

Year 8 – Online -safety

- Understand the various methods employed by hackers to gain personal information (Social engineering)
- Understand how to protect yourself from social engineering methods
- Outline the steps to take if you have any issues surrounding e-safety (DSLs)
- Create an informative newspaper article showing a good understanding of online safety rules

Year 9 (Cyber security - moving towards GCSE level issues)

- Explain the difference between data and information
- Critique online services in relation to data privacy
- Identify what happens to data entered online
- Explain the need for the Data Protection Act
- Recognise how human errors pose security risks to data
- Implement strategies to minimise the risk of data being compromised through human error
- List the common malware threats
- Examine how different types of malware causes problems for computer systems
- Question how malicious bots can have an impact on societal issues

GCSE:

Network Security:

- Explain Malware, Social Engineering, DDOS, Data Interception, SQL injection as forms of attack
- Demonstrate SQL Injection in a controlled environment

- Highlight the importance of Anti-Malware as a common prevention method
- Describe Firewalls as a common prevention method
- Explain the importance of User Access levels as a common prevention method
- Explain the importance of password protection as a common prevention method
- Explain encryption as a common prevention method
- Explain different methods of physical security as common prevention methods
-

EELC (ethical, environmental, legal and cultural) issues

- Describe the impact of ethical, legal, environmental and cultural issues in digital technology within Computer Science
- Explain how the Data Protection Act 2018 impacts on Computer Science
- Explain how the Computer Misuse Act 1990 impacts on Computer Science
- Explain how the Copyright Design and Patents Act 1988 impacts on Computer Science
- Explain the different types of software licences and how they affect Computer Science