Aspire Academy

Online Safety Policy

September 2022

The Local Governing Committee has agreed that this policy will be reviewed every year. This review will take into consideration all aspects of applicable legislation and advice current at the time of the review. The next 'Period of Review' will be ***SEPTEMBER 2023.***

Our Ethos and Values

At Aspire our ethos is to develop the individual moulding independent learners and confident young minds.

We aspire to be a community founded upon mutual trust where everyone is loved and respected for who they are. We believe that in working together we can accomplish more than we could alone.

Values:

As an Alternative Provision Academy, our core values are empathy, courage and community:

- **Empathy** is essential to human life and lies at the heart of all successful relationships. Empathy is an unspoken language that we aim to teach and develop in others. In this way we develop self-awareness and depth of human engagement;

- **Courage** is a trait that needs to be developed in everyone. Life throws many challenges at us and we need to be prepared to face those challenges through developing deep personal reserves. We believe that developing individual strength and conviction enables students for the rest of their lives;

- We aim to be an **inclusive community**. Each person is needed, valued and important. When things go wrong we will forgive each other and make a fresh start. We will share what we have with those in need and try to treat others as we would like them to treat us.

Aims

As an Alternative Provision Academy, we aim to:

- Treat learners, staff and visitors with respect;

- Incorporate and promote the values behind the academy in all we do;

- Instil a sense of self-worth and value in every learner;

- Encourage learner participation in the planning and the running of our Academy wherever possible;

- Encourage emotional literacy as a way of interpreting the world around us;

- Encourage, challenge and support every person to achieve his or her potential.

Introduction

Information and Communication Technology is used increasingly in educational settings, to support teaching and learning as well as playing an important role in the everyday lives of staff and students, both within school and outside.

All schools and academies need to empower children, young people and employees to not only use these technologies safely, but also educate them on the necessary skills to access lifelong learning and employment.

ICT covers a variety of resources including web-based and mobile learning. The technologies that students may use are:

- Websites
- Learning platforms and virtual learning environments
- Emails
- Instant messages
- Chat rooms
- Social networking
- Blogs
- Pod casts
- Downloading music
- Streaming
- Game playing
- Mobile and/or smart phone with text/video/internet access
- Game consoles with internet access
- Other mobile devices with internet access

At Aspire Academy we work to educate our students with regard to 'online' situations. Staff at the Academy discuss and teach the students about appropriate behaviours and work to enable students to remain safe and legal when using the internet and any other related technologies. We think that students need to be provided with guidance, regarding online safety, on a regular and relevant basis. At Aspire Academy we embed online safety throughout the Academy and within the curriculum. We believe it is as important to educate the students as it is to continually refresh staff on potential online issues and how to remain safe and legal online.

This online safety policy is in place to ensure that necessary and relevant measures are embedded to protect students and staff, who are working with ICT equipment and other technologies.

The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and students standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to online safety by knowing the content of the policy and the procedures adopted and developed by the academy.

What does this policy cover?

This policy applies to the whole academy community including the academy's Senior Leadership Team, all staff employed directly or indirectly by the academy, commission partners and all students.

The academy's senior leadership team will ensure that any relevant or new legislation that may impact upon the provision for Online Safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site. This is pertinent to incidents of Online bullying, or other Online related incidents covered by this policy, which may take place outside of the academy, potentially at commissioned provision, but is linked to membership of the academy.

The Academy will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate Online behaviour that takes place outside of the academy.

This Online Safety policy has been written by the Designated Safeguarding Lead, in consultation with the Principal and support and advice from an Online Safety Company and CEOP.

This policy is current and appropriate for its intended audience and purpose.

The School has appointed the DSL to take lead responsibility for Online Safety.

Amendments to the school Online Safety policy will be discussed in detail with all members of teaching staff and training will be given which will link to relevant and current guidance and legislation.

Responsibilities

At Aspire Academy we believe that Online Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for teaching and learning. The following list of responsibilities shows how different members of academy staff will contribute to the academy vision, with regards to Online Safety.

The Senior Leadership Team

The Principal is ultimately responsible for safeguarding provision (including Online Safety) for all members of the academy, with day-to-day responsibility for Online Safety delegated to the Designated Safeguarding Lead (Claire Boyton).

The Principal and Senior Leadership Team are responsible for:

- Ensuring that the DSL and other relevant staff receive effective and up to date training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.
- Ensuring the SLT is updated regularly on online safety issues
- Ensuring procedures are rigorously followed in the event of all Online Safety incidents.
- Receiving timely, regular and routine updates and reports on all Online Safety incidents.
- Ensuring Online Safety education is appropriately embedded across the whole curriculum.

The Designated Safeguarding Lead

The DSL will:

- Promote an awareness and commitment to Online Safety throughout the Academy.
- Be the first point of contact in the Academy for all Online Safety matters.

- Take day-to-day responsibility for Online Safety within the academy and have a leading role in establishing and reviewing the academy Online Safety policies and procedures.
- Have regular contact with other Online Safety committees, e.g. the local authority, Local Safeguarding Children's Partnership (along with the Child Protection Coordinator).
- Will communicate regularly with the academy ICT technician and the academy Senior Leadership Team.
- Will create and maintain Online Safety policies and procedures, reporting to SLT and Governors, at least annually.
- Will ensure that Online Safety is promoted to parents and carers.
- Liaise with the local authority, the Local Safeguarding Partnership and other relevant agencies as appropriate.
- Monitor and report on Online Safety issues to the senior leadership team as appropriate.
- Understand the issues surrounding the sharing of personal or sensitive information.
- Have regular half termly meetings with the Principal – review incidents and the Academy response.
- Understand the dangers regarding access to inappropriate online contact with adults and strangers.
- Be aware of potential or actual incidents involving grooming of children and young people.
- Be aware of and understand Online bullying and the use of social media for this purpose.

Teachers and Support Staff

As a staff team Aspire Academy embraces modern technology but recognises that this is not a right but a responsibility. Sanctions will be used if this expectation is misused

Staff are required to:

- Read, understand and actively promote the Academy's Online Safety policies and guidance.
- Read, understand and adhere to the academy staff Acceptable Use Agreement.
- Ensure that any Online Safety incidents are reported under appropriate escalation routes.
- Develop and maintain an awareness of current Online Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Ensure that any digital communications with students should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social networking etc.
- Embed Online Safety messages in learning activities across all areas of the curriculum.
- Supervise and guide students carefully when engaged in learning activities involving technology.
- Ensure that students are fully aware of research skills and methods.
- Be aware of Online Safety issues related to the use of mobile phones, cameras and Handheld devices.
- Understand and be aware of incident-reporting mechanisms that exist within the academy.
- Maintain a professional level of conduct in personal use of technology at all times.

All Staff and Commissioned Partners

Are required to:

- Be aware of the academy's Online Safety policies and guidance.
- Read, understand and adhere to the academy staff Acceptable Use Agreement.
- Report any Online Safety related issues that come to their attention to the DSL.

- Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in the use of technology at all times.
- Support the academy in providing a safe technical infrastructure to support teaching and learning.
- Ensure that student access to the academy network is only through an authorised, restricted mechanism.

Students
(Shared as part of the Admission Process)

Are required to:

- Understand and adhere to the Acceptable Use Agreement
- Students who are unable to understand the Acceptable Use Policy may require a parent/ guardian to sign on their behalf.
- Help and support the Academy in the creation of Online Safety policies and practices and to adhere to any policies and practices the academy creates.
- Where appropriate students will be expected to understand school policies on the use of mobile phones, digital cameras and handheld devices.
- Know and understand Academy rules relating to bullying and Online bullying.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in the academy and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exist within the Academy.
- Discuss Online Safety issues with family and friends in an open and honest way.
- Through PSHE Lessons and tutor time students will be provided the opportunity to learn about, understand and contribute to the effectiveness of the Online Safety processes.

Parents and Carers
(Shared as part of the Admission Process)

Are required to:

- Help and support the school in promoting Online Safety.
- Read, understand and promote the academy student Acceptable Use Agreement with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children may use within the Academy or at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss Online Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the Academy if they have any concerns about their children's use of technology.
- Sign the photography permission form stating where photographs are to be published upon admission.

Other external groups

- Will receive a copy of this policy.
- The Academy will liaise with other appropriate organisations to establish a common approach to Online Safety and the safe use of technologies.
- Any commissioned provision must reflect this policy in their organisation's practices.
- The conditions of this policy is detailed in conjunction with their SLA
- The Academy will be sensitive and show empathy to internet-related issues
- experienced by students outside of the Academy, for example, social networking sites, and offer appropriate advice where appropriate.

Managing Digital Content

- Before photographs of students can be published, permission must be granted formally and agreed and signed by parents or guardians. All staff should be aware of the process involved with publishing images over different mechanisms.
- Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.
- The Academy will remind students of the risks of inappropriate use of digital images, video and sound in their online activities both at the academy and at home.
- Students and staff will only use Academy equipment to create digital images, video and sound.
- Parents may take photographs at academy events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking.
- When searching for images, video or sound clips, staff will be taught about copyright and acknowledging ownership.

.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the Academy network and never transferred to personally-owned equipment.
- Individual staff members have the responsibility of deleting the images when they are no longer required, or when a student has left the Academy.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for Students' but everyone within the Academy community, lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just in the Academy but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the internet brings.

We recognise that three main areas of Online Safety risk as highlighted by OFSTED are:

1. Content – children and our communities need to be taught that not all content is appropriate or from a reliable source.
2. Contact – Children and stakeholders need to be made aware that digital technologies may be used as a vehicle for grooming, Online bullying and identity theft, and understand how to deal with these risks if they occur.

3. Conduct – Children and parents need to be aware that their personal behaviour online and their electronic identity can increase the likelihood of, or cause harm to themselves and others. Key risk areas being disclosure of personal information, issues around sexting, privacy issues and copyright issues.

In order to minimise these risks to the students at Aspire Academy:

- We will discuss, remind or raise relevant Online Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others.
- Deliver lessons relating to personal safety which can be targeted to vulnerable individuals or groups. This may occur through drop down days or WISK (What I Should Know) sessions as well as the taught curriculum.
- Staff and student computers will have filtering enabled to ensure that inappropriate material is not accessible.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Students will be taught about the impact of bullying and Online bullying and know how to seek help if they are affected by any form of Online bullying.
- Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button. This guidance will be coordinated through the DSL.
- We will provide regular Online safety information to parents and carers.

Staff Training and awareness

- Aspire staff will receive regular information and training on Online Safety issues in the form of regular and routine updates as and when appropriate.
- As part of the induction process all new staff will receive information and guidance on the Online Safety policy and the academy's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the academy community.
- All staff will be required to incorporate Online Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access

(This will be managed by Aspire Academy and Vital)

- The academy will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.

- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- Members of staff will access the network using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow students to access the network through their username and password. They will abide by the academy Acceptable Use Policy at all times.
- Permanent staff will agree removal and return of all e-media at their exit interviews
- All students, when appropriate, will have a unique username and password for access to ICT systems.
- Student and staff use will be monitored and reports generated / followed up where concerns are raised of a safeguarding / misconduct nature.

Passwords

- A secure and robust username and password convention exists for all system access.
- Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- Student passwords will be managed by the appropriate member of support / teaching staff and changed when it is deemed appropriate. Student passwords will be unique.
- Guest logins must be individually allocated and signed for at the main reception.
- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Staff are expected to comply with the following password rules;

    1. Do not write down system passwords.
    2. Never disclose your personal password to anyone. If you think that your password may be compromised, change it as soon as possible. You should regularly change your passwords.
    3. Always use your own personal passwords to access computer based services, never share these with other users.
    4. Make sure you enter your personal passwords each time you log on. Do not include passwords in any automated logon procedures.
    5. Never save system-based usernames and passwords within an internet browser.

New technologies

As an Academy we will keep abreast of new technologies and consider the benefits for both teaching and learning. We will also consider the risks from an Online Safety point of view. We will regularly amend the Online Safety policy to reflect any new technology that we use, or to reflect the use of new technology by students which may cause an Online Safety risk.

The academy will audit ICT equipment usage to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

Mobile phones

As a staff team we embrace modern technology but recognise that this is not a right but a responsibility; therefore students are not allowed to have their mobile phones on them during the school day.

All mobiles will be locked away during the school day and returned to students at the end of the day. Sanctions will be used if this expectation is misused.

Staff use of Mobile Devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional or personal capacity. All staff have access to either an academy mobile phone or main line telephone.
- Staff will use an Academy phone to contact parents or carers within the hours of the school opening times. In exceptional circumstances it may be necessary for members of staff to contact parent/guardians outside of normal working hours. This will be agreed with the DSL.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose. If a member of staff does use a personal device the photos/videos need to be uploaded onto the shared drives and deleted immediately. Senior members of staff needed to authorise this.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Filtering Internet Access

The Academy filters and monitors its internet provision appropriate to the age and maturity of students – filtering is externally managed by Smoothwall and Vital Staff.

- The Academy will always be proactive regarding the nature of content which can be viewed through the academy’s internet provision.
- If users discover a website with inappropriate content, this should be reported to Vital via their email address. This ensures incidents are documented.
- If users discover a website with potentially illegal content, this should be reported immediately to a Senior Leader who will communicate this to the necessary people.
- Any flagged incidents from Smoothwall will be followed up by the Safeguarding Team with the staff or students concerned.
- The Academy will regularly review incidents through the SLT meetings. All concerns can be highlighted to the necessary individuals.
- Students will be taught to assess content as their internet usage skills develop.
- Students will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-academy requirement across the curriculum.

Internet Access Authorisations

- All parents will be required to sign a home-academy agreement during the admissions process. This consent is embedded in a robust admission process whereby appropriate access, internet usage and Online safety is discussed and agreed prior to admission.
- Parents will be asked to read the Academy Acceptable Use Agreement for student access and discuss it with their children, when and where it is deemed appropriate.
- All students will have the appropriate awareness training through Online Safety briefing through the admission process and through lessons. All students are expected to sign the students Acceptable Use Agreement.
- Parents will be informed that students will be provided with supervised internet access appropriate to their age and ability.
- Any visitor who requires internet access will be asked to read and sign an Acceptable Use Agreement. Guest logins are available to those who have signed the acceptable use policy and are associated a personal 'guest' account
- All students will be supervised and monitored during their use of the internet. Students will be frequently reminded of internet safety issues and safe usage.
- Where students are directed to research work at home using the internet, parents / carers will be informed of the nature / type or specific websites being used.

Email

Staff are required to comply with the following:

- Staff should only use approved email accounts allocated to them by the Academy and should be aware that use of the academy email system is monitored and checked.
- Staff should not use personal email accounts during Academy hours or for professional purposes, especially to exchange any academy-related information or documents.
- Access, within the Academy, to external personal email accounts may be blocked.
- The Academy gives all staff their own email account to use for all Academy business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff are responsible for keeping their password secure.
- Under no circumstances should staff contact students, parents or conduct any academy business using personal email addresses.
- Irrespective of how staff access their academy email (from home or within the academy), Academy policies still apply.
- All emails that are no longer required or of any value should be deleted.
- Staff should check email accounts regularly for new correspondence.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source.
- Communication between staff and students or members of the wider academy community should be professional and related to school matters only.
- Any inappropriate use of the Academy email system or receipt of any inappropriate messages from another user should be reported to a senior member of staff immediately.
- All email users within the Academy should report any inappropriate or offensive emails through the Local Authority incident-reporting system.

Use of Social Media

- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff and students are asked to report any incidents of Online bullying to the academy.
- Staff will raise any concerns about a students' use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.
- All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Agreement.
- Staff must not use social media tools to communicate with current or former students.
- Staff will not use any social media tools to communicate with parents.
- Procedures for dealing with Online bullying incidents of staff or students involving social media are outlined in the academy Anti-Bullying policy.
- Staff are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.

Electronic Bullying and harassment

This Online safety policy recognises the additional dangers of online bullying. All staff and Students' should be aware that any misuse of ICT to bully or harass others will be dealt with under the academy Anti Bullying policy, and are reminded that:

'Bullying is behaviour by an individual or group, repeated over time, which intentionally hurts another individual or a group physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages or the internet), and is often motivated by prejudice against particular groups (for example on grounds of race, religion, gender, sexual orientation, or because a child is adopted or has caring responsibilities). It might be motivated by actual difference between children, or perceived differences. Stopping violence and ensuring immediate physical safety is obviously a first priority but emotional bullying can be more damaging than physical. All staff will have to make their own judgements about each specific case.'

Dealing with incidents

All Online Safety incidents at Aspire Academy are logged and recorded on management systems, with procedures regularly audited by the Principal and the Vice Principal. All staff must ensure that the needs and sensitivities of the student should be at the forefront of whatever the issue, and any action(s) should support the student or students involved, whilst adhering to existing academy policies and current legislation.

Staff need to be aware of the following issues:

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Designated Safeguarding Lead and the Principal who will refer this to appropriate external authorities such as the Police, CEOP, Internet Watch Foundation or other agencies as appropriate. Examples of illegal offences are:

- Accessing Child abuse images
- Accessing criminally obscene content
- Inciting racial hatred

- Accessing sexual child abuse images and content

Staff should never under any circumstances investigate, interfere or share evidence of these activities as they may themselves be committing an illegal offence in doing so.

Inappropriate use

Staff and students at the Academy are likely to have to deal with ‘accidental’ access to inappropriate materials and content. Examples of these and the actions and sanctions to apply are as follows:

1. Accidental access to inappropriate materials. Recommendation is to minimise the application, turn off the monitor. Students should tell a trusted member of staff. Staff will enter the details on a red slip, and notify the Designated Safeguarding Lead who can then notify the filtering and monitoring company.
2. Using another person’s logins, accounts or passwords
3. Deliberate searching for inappropriate materials
4. Bringing inappropriate electronic media into the academy
5. Inappropriate use of chat and forums.

Recommendation for each of the above is to inform the Designated Safeguarding Lead or Assistant, enter the details onto the incident log, re-iterate and raise Online Safety issues with the individual or class, and for more serious or persistent offences consider disciplinary action and parent/ guardian involvement.

Evaluating the impact of this Online Safety Policy

The SLT will regularly and routinely monitor and evaluate the impact of this policy by monitoring the number and range of Online Safety incidents in the school, regularly testing and checking on students awareness of Online Safety issues and looking for patterns and trends in practice.

The policy will be reviewed on an annual basis. External agencies will be used to support this, to ensure current trends, new and emerging technologies and new threats to student safety are captured when the policy is refreshed.

This policy should be read in conjunction with other relevant safeguarding policies such as:

- Safeguarding and Child Protection Policy
- Health and Safety Policy
- Staff Code of Conduct
- Anti-Bullying Policy
- Staff Induction Policy
- Behaviour Policy

Who do I contact if I have any issues?

If you have any concerns regarding online safety please contact the academy on 01482 318789, and speak to a Student Liaison Officer or the Designated Safeguarding Lead.

You can also contact:

Designated Safeguarding Lead/Child Protection officer: Claire Boyton Vice Principal – cboyton@asp.hslt.com

Deputy Safeguarding Lead/Child Protection Officer: Maxine Lane – Child Protection Officer mlane@asp.hslt.com