E-safety Policy

2023-2024

Scope

This policy applies to all members of the academy community (including staff, students, volunteers, parents, carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the Academy.

The use of technology has become a significant component highlighting many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establish mechanisms to identify, intervene in, and escalate any incident where appropriate. E-safety should form a fundamental part of schools' and colleges' safeguarding and child protection measures.

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 academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place both inside and outside of school.

Internet Safety

The internet can offer educational and social benefits to students and adults with technologies such as mobile phones, tablets, computers and games consoles. However, it is also important to consider the risks associated with these technologies, students could unknowingly expose themselves to

danger, and adults could be a target for identity theft. Comments posted on social networking sites have led to students being bullied and staff being disciplined.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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 scams.

Roles and Responsibilities

The academy will take all reasonable precautions to ensure e-Safety. However, owing to the scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The Academy cannot accept liability for material accessed, or any consequences of, internet access.

Staff responsible for E-Safety:

- The members of staff responsible for e-safety at Blackpool Aspire Academy are Mrs Rawson, Assistant Headteacher and Designated Safeguarding Lead as well as Miss Markham, Lead Caseworker, Mr Sheldon, Senior IT Technician who will:
    - take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
    - ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
    - provides training and advice for staff
    - liaises with school technical staff
    - attend relevant meetings
    - monitor all violations and concerns using filtering and monitoring software, Senso Cloud
    - action any violations and concerns via existing safeguarding systems and the behaviour policy.

The Academy will:

- Provide a safe environment for students and staff.
- Ensure all students know how to report an e-safety/safeguarding concern
- Block/ filter access to social networking sites and other inappropriate websites.
- Advise students never to give out personal details of any kind that may identify them or their location.

- Monitor internet usage via Senso Cloud and report any inappropriate use to Designated Safeguarding Lead and IT Technician using establish safeguarding reporting systems.

Staff will:

- Staff accept that the Academy can monitor internet usage to help ensure staff and student safety.
- Confiscate items such as their mobile devices and smart technology. This will occur when they are being used during the school day which may contravene the school behaviour/anti-bullying policy.
- Report anything inappropriate they find on the internet.
- Websites used will be viewed by staff prior to any lessons.
- Staff should not be accessing the internet for personal reasons while teaching students. Students will:
- Only use approved e-mail accounts on the school network.
- Must immediately report if they see any inappropriate material.
- Must not reveal personal details of themselves or others.
- Must not intentionally view inappropriate material on any device.

Monitoring Provider – Senso Cloud

The following information explains how Senso Cloud meets the national defined 'appropriate monitoring' standards:

Monitoring Content:

- Senso is a member of the IWF and actively communicates with them.
- Senso blocks IWF URLs (utilisation of IWF URL list for the attempted access of known child abuse images) and logs attempted access, without sharing the URL details or taking screenshots.
- Senso blocks access to CTIRU (the police assessed list of unlawful terrorist content, produced on behalf of the Home Office) unlawful terrorist content.

Inappropriate Online Content:

- Illegal - content that is illegal, for example child abuse images and unlawful terrorist content.
- Bullying - involves the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
- Child Sexual Exploitation - is a child being encouraged into a coercive/manipulative sexual relationship. This may include encouragement to meet.
- Discrimination – which promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity
- Drugs/substance abuse - displays or promotes the illegal use of drugs or substances.
- Extremism – which promotes terrorism and terrorist ideologies, violence or intolerance.
- Pornography – displays of sexual acts or explicit images.
- Self-harm – that promotes or displays deliberate self-harm.
- Suicide - suggests the user is considering suicide.
- Violence - Displays or promotes the use of physical force intended to hurt or kill.

Monitoring System Features:

- Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
- Multiple language support - Senso is based on Unicode characters which allows us to support any language including those with non-Latin alphabets
- Alerts are generated and prioritised to enable a rapid response to immediate issues.
- Remote monitoring - students are able to be monitored regardless of their location as long as they have an internet connection.
- Harmful Image detection - Upon a keyword violation capture and screenshot, Senso Safeguard Cloud will analyse the screenshot using AI-driven threat detection. The AI system is trained to determine whether the screenshot contains images that match the following categories: - Alcohol - Drugs - Extremism - Gore - Porn - Swim/Underwear - Weapons

Education

E-safety at Blackpool Aspire Academy is focused in all areas of the curriculum and staff reinforce e-safety messages across the curriculum.

- A planned e-safety curriculum is provided as part of Digital Technology, the Personal Development Programme such as PHSE and other lessons and is a topic that is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies, Aspirational Days and form tutor time as part of the Personal Development Programme.
- Students are taught in lessons to be critically aware of the materials or content they access on-line and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and we have processes in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.

Staff

- All staff receive ongoing e-safety training, which is regularly updated.
- Staff also receive a monthly e-safety newsletter.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- The E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice and training to individuals as required.

Parents and Carers

The academy will seek to provide information and awareness to parents and carers through:

- Curriculum activities
- E-safety newsletter (monthly), letters, e safety updates Parents and carers evenings
- A dedicated e-safety section on the website for parents and carers
- Reference to the relevant web sites / publications
- Phone calls to parents/carers when e-safety incidents have occurred.

Sanctions

Whenever a student commits an e-safety offence, the incident will be dealt with by recording it as an 'E-Safety Incident' in our behaviour reporting tool ClassCharts and also as a safeguarding concern in Safeguard My School.

If a staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Senior Leadership Team/Headteacher.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. ClassChart points, certificates, class commendation for good research skills, certificates for being good cyber citizens etc.

Monitoring and reporting

- The impact of the e-safety policy and practice is monitored through the audit of e-safety incident logs, behaviour logs, surveys of staff, students, parents and carers
- The records are audited and reported to:
  the academy's senior leaders
  The academy council
  FCAT safeguarding board
- This policy will be reviewed every year. The next review is due September 2024.
- This policy should be read alongside the Anti-bullying Policy, Behaviour Policy and Safeguarding Policy.

Government Advice

The government have produced 'Advice for parents and carers on cyberbullying':

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf

For further help and support you can access the following pages or the e-safety section on the academy website:

https://www.thinkuknow.co.uk/

http://www.bullying.co.uk/cyberbullying

http://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx

https://www.nationalbullyinghelpline.co.uk/cyberbullying.html