Fylde Coast Academy Trust

(FCAT)

Online Safeguarding Policy and Management Systems V3

Policy Version & Issue Date	Version 1 First Version – February 2017
Policy Version & Issue Date / review / summary	Version 2 February 13th 2019
Policy Version & Issue Date / review / summary	Version 2 December 12th 2021
Electronic copies of this plan are available from	FCAT / Academy Website
Hard copies of this plan are available from	FCAT / Academy
Date of next review	December 2024 / as required
Person/s responsible for review	Simon Brennand

Associated Documents:

FCAT Equality Policy

FCAT Safeguarding Policy

FCAT Preventing Extremism and Radicalisation Policy

Scope

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

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 FCAT to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other online safeguarding incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

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.

FCAT will deal with such incidents using strategies and procedures outlined within this policy, the academy Behaviour Policy and Anti-Bullying Policy and will (where known) inform parents or carers of incidents of inappropriate online behaviour that has taken place. This policy describes the management systems and arrangements in place to create and maintain a safe learning environment for all our children, young people and staff. It identifies actions that should be taken.

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 can lead to students being bullied and staff being disciplined and are unacceptable.

Risks associated with the internet, mobile devices and social networking sites include:

• Cyber bullying
• Radicalisation and Extremism and inclusion of the Prevent Duty
• Grooming
• Potential abuse by online predators
• Identity theft
• Exposure to inappropriate content
• Racist
• Hate
• Pornography

Roles and Responsibilities

FCAT will take all reasonable precautions to ensure online safeguarding. Please note that 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 an academy computer or mobile device. FCAT cannot accept liability for material accessed, or any consequences of, internet access.

The FCAT ICT Strategic Lead will scope and lead the implementation of network-wide safeguarding systems, such as network monitoring.

The Academy Online Safeguarding Lead will:

• lead the development of online safeguarding strategy
• take day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the academy online safeguarding policies / documents
• ensure that all staff are aware of the procedures that need to be followed in the event of an online safeguarding incident taking place.
• provide training and advice for staff
• liaise with the Academy Board and FCAT Safeguarding Board as required
• liaise with academy technical staff
• receive reports of online safeguarding incidents and maintains a log of incidents to inform future online safeguarding developments, meet regularly with the (online) Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
• attend relevant meetings
• report regularly to Senior Leadership Team

The Academy Council / Online Safeguarding Governor will:

• meet with the Online Safeguarding Co-ordinator
• monitor online safeguarding incident logs
• monitor network filtering, monitoring and change control logs
• report to Academy Board and FCAT Safeguarding Board

The Academy will:

• Provide a safe environment for students and staff.
• Block/filter access to social networking sites/inappropriate websites.
• Advise students never to give out personal details of any kind that may identify them or their location.
• Monitor internet usage and report any inappropriate use to pastoral colleagues and/or the DSL.

Staff will:

• Accept that the academy can monitor internet usage to help ensure staff and student safety.
• Confiscate items such as mobile phones, iPods or other digital devices if they are used in school and/or to contravene the school Behaviour and/or Anti-Bullying policy. (See Portable Digital Device Policy)
• Report anything inappropriate they find on the internet.
• View websites to be used prior to any lessons.
• Behave professionally and in accordance with the FCAT Code of Staff Conduct when online
• Not access the internet for personal reasons when teaching students.

Students will:

• Only use approved e-mail accounts on the academy network.
• Immediately tell a teacher / member of staff if they see any inappropriate material.
• Not reveal personal details of themselves or others online.
• Not intentionally view inappropriate material on any device.

Education

Students

Online safeguarding is focused in all areas of the curriculum and staff will reinforce online safeguarding messages through a range of learning opportunities in different subject areas.

• A planned online safeguarding curriculum is provided as part of Computing, PHSE and other lessons and is regularly revisited
• Key online safeguarding messages are reinforced as part of a planned programme of assemblies and pastoral activities
• 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 the academy
• Staff are to 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 processes are in place to deal 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 (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technical Team 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
• The online safety committee will include student representation
• Student digital experts will be deployed

Staff

A planned programme of formal online safeguarding training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safeguarding training needs of all staff will be carried out regularly. It is expected that some staff will identify online safeguarding as a training need within the performance management process.

• All new staff will receive online safeguarding training as part of their induction programme, ensuring that they fully understand the FCAT Online Safeguarding Policy and Acceptable Use Agreements.
• The Online Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
• The Online Safeguarding Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
• The Online Safeguarding Lead will provide advice and training to individuals as required.

Governors

• Attendance at training provided by FCAT, National Governors Association or other relevant organisations.
• Participation in academy training/information sessions for staff or parents.

Parents and Carers

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

• Curriculum activities
• Letters, newsletters, online safety updates and websites
• Parent and carer safeguarding awareness raising opportunities
• Reference to the relevant websites/publications

Sanctions

Whenever a student or staff member infringes the Online Safeguarding Policy, the final decision on the level of sanction will be at the discretion of the academy / FCAT leadership. The following are provided as examples:

Students

Level 1 infringement

• Use of non-educational sites during lessons
• Unauthorised use of email
• Unauthorised use of mobile phone (or other technologies)
• Use of unauthorised instant messaging/social networking sites

(Possible Sanctions: referred to Faculty/Department Leader, Online Safeguarding Lead, confiscation of phone)

Level 2 infringement

• Continued use of non-educational sites during lessons after being warned
• Continued unauthorised use of email after being warned
• Continued unauthorised use of mobile phone
• Continued use of unauthorised instant messaging/social networking sites
• Use of file sharing software
• Accidentally corrupting or destroying others' data without notifying a member of staff of it
• Accidentally accessing offensive material and not notifying a member of staff.

(Possible Sanctions: referred to Faculty/Department Leader, Online Safeguarding Coordinator, removal of Internet access rights for a period, confiscation of phone and contact with parent)

Level 3 infringements

• Deliberately corrupting or destroying someone's data, violating privacy of others
• Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
• Deliberately trying to access offensive or pornographic material

(Possible Sanctions: referred to Faculty/Department Leader, Online Safeguarding Coordinator, Headteacher, removal of internet rights for a period)

Level 4 infringements

• Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act and/or GDPR
• Bringing the academy or FCAT into disrepute

(Possible Sanctions – Referred to SLT and/or Headteacher, contact with parents, possible exclusion, referral to DSL and/or the Police)

Other safeguarding actions:

• Secure and preserve any evidence
• Inform the sender's e-mail service provider if a system other than the academy system is used. Students are also to be informed that sanctions can be applied to online safeguarding incidents that take place out of academy day if they are related to an academy

Staff

Level 1 infringement (Misconduct)

• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
• Misuse of first level data security, e.g. wrongful use of passwords
• Breaching copyright or license e.g. installing unlicensed software on network

Sanction – Referral to the Headteacher, FCAT disciplinary procedures

Level 2 infringement (Gross Misconduct)

• Serious misuse of, or deliberate damage to, any academy computer hardware or software;
• Any deliberate attempt to breach data protection or computer security rules;
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 and/or GDPR;
• Bringing the FCAT / academy name into disrepute.

(Sanction – Referred to Headteacher/Academy Council and follow school disciplinary procedures; report to FCAT HR)

Other safeguarding actions:

1. Remove the device to a secure place to ensure that there is no further access.
2. Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

Rewards

Recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms, for example class commendation for good research skills, certificates for being good cyber citizens.

Monitoring and reporting

1. The impact of the Online Safeguarding Policy and practice is monitored through the audit of online safeguarding incident logs, behaviour logs, and surveys of staff, students, parents and carers

2. The records are audited and reported to:

• the academy's senior leaders
• The Academy Council
• FCAT Safeguarding Board
• Blackpool Safeguarding Children Board (BSCB)

The academy action plan indicates any planned action based on the above.

3).For further help and support you can access the following pages:
http://ceop.police.uk/safety-centre/11-16/
http://www.bullying.co.uk/cyberbullying/
http://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx