Ark John Keats Academy

# E-Safety Policy

| | | | |
|---|---|---|---|
| Date of last review: | September 2020 | Review period: | 2 years |
| Date of next review: | September 2022 | Owner: | Jo Facer |
| Type of policy: | Network | | |

Updated: Sept 2020

## POLICY INFORMATION

### Named personnel with designated responsibility:

| Academic year | Designated Senior person | Deputy Designated Senior person | Nominated Governor | Chair of Governors |
|---|---|---|---|---|
| 2020/2021 | D.Sufi | | | Linsey Cole |

### Policy review dates

Frequency of review: annually

| Review | Changes made | By whom |
|---|---|---|
| Sep 2020 | Policy Updated | Deega Sufi |

# Contents

**Named staff with designated responsibility for E-Safety**

| Principal | Designated Safeguarding Lead | Deputy Designated Safeguarding Lead | Nominated Safeguarding Link Governor | Chair of Governors | Local Authority Designated Officer (LADO) |
|---|---|---|---|---|---|
| Jo Facer | Marne Reynecke (Primary)<br>Deega Sufi (Secondary) | Bradley Davis<br>Lydia Socrates | Christopher Jones | Lindsey Cole | Bruno Capela |

# 1. Introduction

1.1 E-safety covers issues relating to children and young people and their safe use of not only the Internet, but also other electronic communications such as mobile phones, both in and out of the academy. It includes education on risks and responsibilities and is part of the duty of care which applies to everyone working with children, while still promoting the use of the internet and technologies as an important tool for education and communication. As use of technology is now universal – pupils interact with new technologies such as mobile phones and the Internet on a daily basis – it is imperative that they learn skills to prepare themselves for the working environment.

1.2 E-safety concerns safeguarding children and young people in the digital world, where the risks associated with new technologies can be grouped into four main categories – content, contact, commerce and culture.

1.3 Content – Much of the material on the Internet is published for an adult audience and some is unsuitable for young people. In addition, there is information available on line on weapons, crime, racism, suicide, extremism, pornography and other inappropriate material which may be more restricted elsewhere.

Contact – The Internet is an unmanaged, open communications channel, with a variety of ways to transmit information internationally at low cost. Adults can abuse this in order to groom young people with a view to sexually abusing them. Young people may not be aware of the danger of publishing or disclosing personal information and so may put themselves of other young people at risk. In addition, young people may not have the maturity to communicate appropriately with their peers via an online medium.

Commerce – Young people are vulnerable to engaging in transactions which may have serious financial consequences.

Culture – Pupils must be taught to use new technologies responsibly, so as to not become involved in the above, but also to avoid breaching copyright or plagiarising. In addition a risk to consider is obsessive use of the Internet having an adverse effect on health, social and emotional development.

1.4 The will ensure that an Acceptable Use Policy is in place for staff and pupils and that e-safety is both embedded in the curriculum for pupils and the CPD programme for staff. This policy will be continually reviewed in response to the growing and changing nature of new technologies. This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet

and other communications technologies for educational, personal, and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

## 2. The purpose of this document

2.1 The purpose of the following document is to promote the use of new technologies within the curriculum, while also safeguarding pupils from harm associated with those new technologies. It also seeks to protect staff in their contact with pupils and their own use of the internet by providing clear expectations for staff and pupils on acceptable use of the internet. This document will work in conjunction with other academy policies including the Behaviour policy, the PSHE policy and the Safeguarding policy. It has been written by the academy, building on the Enfield e-Safety guidance. It has been agreed by the senior leadership team and approved by the governors.

2.2 This policy will be annually reviewed in response to the growing and changing nature of new technologies and the laws and legislation that reflect these. The responsibility for this review will fall to the designated safeguarding lead.

## 3. Teaching and learning

3.1 As use of technology is now universal – pupils interact with new technologies such as mobile phones and the Internet on a daily basis – it is imperative that they learn skills to prepare themselves for the working environment. The role of the Internet and other new technologies in the academy is therefore to raise educational standards in order to promote pupil achievement and to support the professional work of staff. In addition, pupils will engage with the Internet widely outside of the academy and will need to learn both how to keep themselves safe, behave appropriately in a virtual environment and also how to evaluate information found online.

3.2 In the academy Internet access will be designed expressly for pupil use, including filtering appropriate to the age of the pupils. Where appropriate, pupils will be restricted from using search engines, but instead directed to previously approved websites selected to enhance learning.

3.3 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use within lessons. To support this, all pupils will sign an acceptable use agreement as part of their induction to the academy.

3.4 Pupils will be explicitly taught to effectively use the Internet for research in a way that respects copyright and intellectual property rights in a way that is age appropriate.

3.5 In addition, critical evaluation of the quality of materials found online should be taught when age appropriate. Opportunities to develop these skills will be built into the curriculum across all subjects, including the appropriate way to reference resources found online.

## 4. Managing Information Systems

4.1 The responsibility for managing the security of the academy ICT systems falls to the Ark

Central IT team, including the onsite technicians employed by Ark. The security of the academy information systems will be reviewed regularly, with regular virus protection updates.

4.2 E-mail is an essential means of communication for both staff and pupils. Pupils may only use approved e-mail accounts in the academy so that they can be regulated. Pupils will be told as part of their e-safety education that if they receive an offensive e-mail they must immediately report it to a teacher or an appropriate member of SLT. Staff should only use academy email accounts to communicate with parents or pupils, including a dedicated email account for reporting wellbeing and pastoral issues, monitored by those staff responsible for pastoral care. Staff also use Impero Edaware to report safeguarding concerns confidentially.

4.3 The academy website is a resource intended to open communication channels with parents, pupils and the surrounding community, as well as celebrating success of the academy and pupils. Sensitive information about the academy will be protected on the website by ensuring that the personal information of staff and pupils is not published on the website. In addition, any images used on the website will adhere to the images policy of the academy.

4.4 All staff and pupils will be made aware of the potential risks of using social media sites and informed of methods to protect themselves as part of the ongoing e-safety education provided by the academy. All social networking sites will be blocked on the academy internet. Any websites or online resources used by staff and pupils will be either password protected or restricted in the use of personal information.

4.5 Levels of internet access and supervision will vary according to the age and experience of the pupils. In general, blocking strategies will be utilised to prevent access to unsuitable sites. If staff or pupils discover unsuitable sites they will be advised to report the URL to the appropriate member of staff.

4.6 Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in the academy is allowed. Any new technology use in the classroom will have educational merit. Mobile phones will not be allowed in the academy, but will rather be collected in at the beginning of each day and redistributed to pupils at the end of the school day in named bags.

4.7 Personal data held by the academy will be recorded, processed, transferred and made available according the Data Protection Act 2018.

# 5. Policy Decisions

5.1 The academy will maintain a current record of all staff and pupils who are granted access to the academy's electronic communications. All staff and pupils must read and sign the appropriate usage agreement before using any academy ICT resource. At KS1, access to the internet will be by adult demonstration only, unless directed to specific, approved on-line materials.

5.2 The academy will take all reasonable precautions to ensure that users access only appropriate material. The academy uses a filtering system called Senso, and LGFL for monitoring IT websites and access which blocks inappropriate content being accessed. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via an academy computer. The academy does not accept liability for the material accessed, or any consequences resulting from internet use. Methods to identify, assess and minimize risks will be reviewed regularly.

5.3 Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint

about staff misuse must be referred to the principal. All incidents will be recorded in the academy e-safety log, with all sanctions following the academy behaviour policy.

5.4 Cyber-bullying will not be tolerated in the academy. Full details are set out in the academy's anti-bullying policy. Sanctions for those involved in cyber-bullying may include:

- Removing offensive material.
- Suspension of internet rights in the academy.
- Parent/carer contacted.
- The police will be contacted if a criminal offence is suspected.

5.5 E-safety training for pupils will be embedded into the character programme, and in all subjects when appropriate. In addition, e-safety rules will be posted in rooms with internet access and all pupils informed that network and internet use will be monitored.

5.6 All staff will be given access to the academy e-safety policy and its application and importance explained. In addition the e-safety policy will be available on the academy website. To protect all staff and pupils, Acceptable Use Policies will be implemented. Staff and pupils do not have access to the school Wi-Fi and network on personal phones, however staff are permitted in using personal mobile devices to access emails and Microsoft Teams. Staff cannot store or download school data on personal devices and must inform Ark central if there is a data breach.

5.7 The school will inform and educate users about risks on the use of digital and video images, and will implement policies to reduce the likelihood of the potential for harm:

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- Staff are allowed to take digital / video images to support educational aims using school owned devices, 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images, and have consent.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

# 6. E-safety education - Primary

6.1 E-safety education will be provided in the following ways across Primary and Secondary:

- E-Safety advice is provided as part of the class teacher/form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum.
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are encouraged to adopt safe and responsible use of ICT, the Internet, and mobile devices both within and outside of school during designated lessons and curriculum areas.
- Pupils are taught about e-safety in the context of extremism and radicalisation and Child Sexual Exploitation.
- Rules for the use of ICT systems and the Internet are made clear and available to pupils
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

6.2 Pupils will be educated that they should think carefully before visiting any site, even if recommended to them by a friend or an older person. They will be told they must not upload photographs of themselves or other pupils to any sites, and must not publish any personal information including location and contact details. Pupils must be educated in how to communicate safely online, especially those who are vulnerable due to social isolation.

Pupils should be taught that if they do see images or content online which distresses them that they should close or minimise the window immediately and inform an adult. Best practice would suggest that the site is not closed so that it can be reported by an appropriate adult as necessary. If an incident occurs in school, parents should be notified if appropriate. All incidents should be recorded in the e-safety log.

6.3 At KS1, nearly all online learning should be directed by the teacher. For KS2 pupils, use of online search engines should be carefully considered. Pupils should normally be referred to previously approved websites.

6.4 E-safety education in the classroom will be based around the CEOP resources, in line with Enfield recommendations. Teaching resources can be found at www.thinkuknow.co.uk.

6.5 E-safety strategies should be applied to the entire cohort of pupils, but with particular consideration to vulnerable pupils as outlined below:

| Content | Contact | Conduct |
|---|---|---|
| **Students who:**<br>• Have inconsistent supervision and limited parent/carer awareness in home settings.<br>• Don't understand the hidden/true meanings of inappropriate advertising or language.<br>• Find it difficult to explain experiences verbally. | **Students who:**<br>• Have limited understanding of online risk.<br>• Have poor understanding of social uses of language for humour, sarcasm, compliments or street talk.<br>• Are socially isolated children and young people.<br>• Look for support in potentially inappropriate Internet forums. | **Students who:**<br>• Find it difficult to stop and think about consequences of their actions.<br>• Don't perceive that they have broken 'netiquette' rules.<br>• Don't understand how to respond to coercion.<br>• Don't have adequate literacy skills to understand written rules and sanctions. |

# 7. E-safety education – secondary

7.1 E-safety lessons are delivered to all pupils through character sessions. The content covered

is age appropriate and addresses various topics such as online safety, safer internet use and social networking. Pupils revisit the online safety module in KS3, KS4 and KS5. When using digital images, staff should inform and educate pupils 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. An integral part of e-safety education for older pupils at the academy will revolve around equipping them with the tools to cope with inappropriate material that they may come across. In addition, pupils will be made aware that they are in large responsible for their own safety when using online resources.

7.2 Pupils will also be educated in how to interact with the internet responsibly in line with Think U Know training, in line with the Enfield recommendation. They will be trained to become critically aware of resources that they find online and to respect copyright when using Internet material in their own work. Online Safety information is also on the safeguarding posters around the school for pupils to access CEOP information.

7.3 Access in the academy will be on the basis that secondary pupils have agreed to an Appropriate Use policy. The academy will take the responsibility to provide the appropriate level of web filtering and safe search. The academy will remove this privilege should a good reason arise.

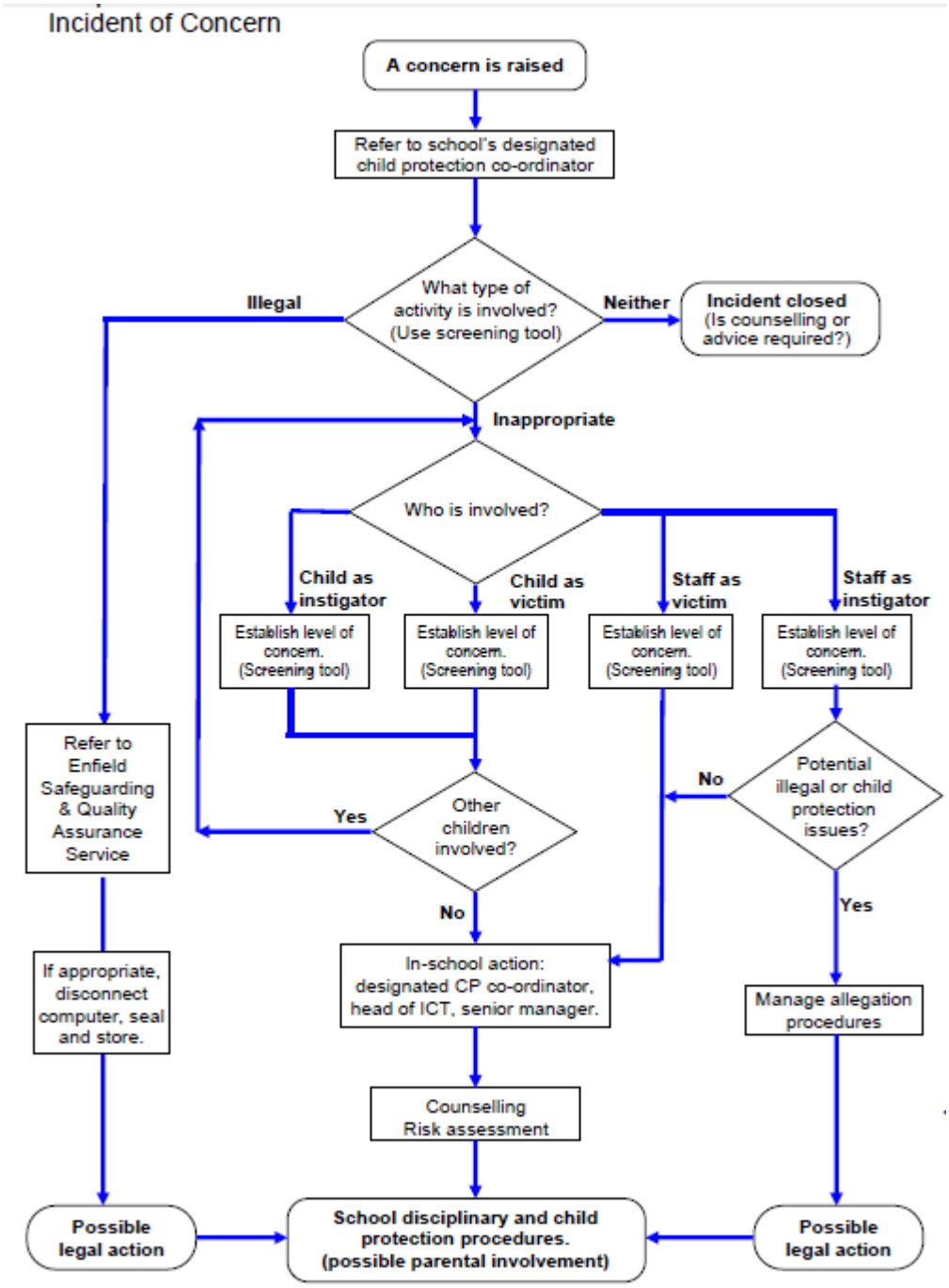
# 8. Responding to an incident

8.1 The risks that could be posed to young people and adults when online are as follows:

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

8.2 Following any incident, the following procedure will be followed:

- All incidents recorded in the e-safety log and other relevant areas as necessary.
- All appropriate staff members informed and behavior policy adhered to where appropriate.
- If necessary, incident referred on to appropriate external colleagues including the police if necessary
- The flow chart below can be used to decide on appropriate procedure to follow.


Incident of Concern
A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Enfield Safeguarding & Quality Assurance Service
Other children involved?
Yes
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action