All Saints National Academy

E-SAFETY POLICY

Policy Review

This policy will be reviewed in full by the Governing Body on an annual basis.

The policy was last reviewed and agreed by the Governing Body on 26/01/20

It is due for review on 26/01/21 (up to 12 months from the above date).

Signature ……. Date ……

Principal

Signature ……. Date ……

Chair of Governors

1. POLICY INTRODUCTION

At All Saints National Academy we endeavour to help everyone achieve their potential. By listening to each other, thinking about what we do, checking our outcomes and always striving to improve we will ensure that everyone can be safe, happy and successful.

2. POLICY STATEMENT

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other academy policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The academy must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

3. POLICY INTENT

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the academy ICT systems, both in and out of the academy.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils 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 out of the academy, but is linked to membership of the academy.
The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of the academy.

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the academy's e-safety provision. Children and young people need the help and support of the academy to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside the academy
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in the classrooms and around the site
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Academy ICT systems will be managed in ways that ensure that the academy meets the e-safety technical requirements outlined in any relevant Local Authority and/or Trust E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of the academy ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the academy ICT systems
- All users will be provided with a username and password

Users will be made responsible for the security of their username and password, 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.
Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.
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 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

- Staff are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy 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 academy 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 students / pupils will be selected carefully and will comply with GDPR with regards the use of such images
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the academy website
- Pupil's work can only be published with the permission of the pupil and parents or carers

When using communication technologies the academy considers the following as good practice:

- The official academy email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in the academy, or on academy systems
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat etc) must be professional in tone and content
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the academy and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The academy believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in the academy or outside the academy when using academy equipment or systems. The academy policy restricts certain internet usage as follows:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute
- using academy systems to run a private business
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- on-line gaming (educational)
- on-line gaming (non educational)
- on-line gambling
- on-line shopping / commerce
- file sharing
- use of social networking sites
- use of video broadcasting eg Youtube

APPENDIX 1 Internet Safety and the use of Social Media – Year 5 & 6

All Saints National Academy is committed to promoting the safe and responsible use of the internet and as such we feel it is our responsibility to raise this particular issue, due to the increase in inappropriate use of Skype, Snapchat, Instagram, Facebook and group games such as Fortnight. Many of the issues that have been brought to our attention recently have involved the use of:

• Skype - a video and messaging app. You are required to be at least 13 years old before you can create an account

• Snapchat - a photo and video sharing app allowing images and texts to be sent and automatically deleted after a set amount of time. You are required to be at least 13 years old before you can create an account

• Instagram - an online mobile photo sharing, video sharing and social networking service which enables its users to take pictures and videos and share them on a variety of social networking platforms. You are required to be at least 13 years old before you can create an account

• Facebook - a social networking site. You are required to be at least 13 years old before you can create an account

• WhatsApp – An instant messaging app for smartphones. The user agreement requires users to be age 16 or older. Children are often creating 'groups' to which others are joining. This means that all information is shared with anyone who is in the group so privacy is lost and in some cases strangers have been added to the group

• Fortnight - a group game where children can be muted and excluded from groups. The recommended age for this game is 13 years

• TikTok – a video sharing social networking service which lets users create, share, and view user created videos much in a similar manner to Facebook, Instagram and Snapchat. Users have to be 13 to sign up

We understand that it is increasingly difficult to keep up with the ways that our children are using new and ever changing technologies. Our children are immersed in a society that has become dependent on powerful computers, including smart phones, iPads, interactive online games and virtual communities.

Websites such as Facebook, Instagram, Skype and WhatsApp to name but a few, offer fantastic opportunities for communication and social connections, however they are created with their audience in mind especially sites such as Facebook and Instagram which are specifically for those over 13 years old. When monitoring your son/daughter's internet use, please remind yourself of the concerns of social media:

• Many sites use 'targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated when they registered. They may have lied about their age to get an account, making them appear older than they are, increasing this risk.

• Young people may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour. The general rule is, if they aren't friends in real life, they shouldn't be 'friends' online
• Language, games, groups and content posted or shared on social media is NOT moderated, and therefore can be offensive, illegal or unsuitable for young people
• Photographs shared by users are NOT moderated and therefore young people could be exposed to inappropriate images or even post their own
• Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options
• Social media sites can be exploited by bullies and for inappropriate contact
• Social media sites cannot and do not verify its members, therefore, it is important to remember that if your son/daughter can lie about who they are online, so can anyone else
Primarily, these occurrences and reported incidents of misuse of social media sites happen at home, after academy hours when children have access to web sites that are blocked in the academy. With this in mind, and in response to concerned parents who have asked for advice regarding internet safety, we feel it important to point out to parents the risks of unregulated use of such sites, so you can make informed decisions as to whether to allow your child to have a profile or not and when and how to monitor their use, particularly at night time. We strongly advise a device free bedroom policy after bedtime to allow for uninterrupted sleep and rest.
Although we cannot govern matters occurring out of academy hours which is parental responsibility, we will take action (such as reporting under age profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils, including reporting the use of inappropriate images of young people to the police, as this is a legal matter. This also refers to inappropriate text messages.

Should you decide to allow your child to have an online profile we strongly advise you:
• Check their profile is set to private and that only their friends can see information they post
• Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting or messaging offensive /inappropriate messages or photos
• Monitor your child's use of language and how they communicate to other people, ensuring profanity is discouraged
• Have a look at advice for parents on the social media sites
• Set up your own profiles so you understand how the site works and ask them to have you as their friend on their profile so you know what they are posting online
Make sure your son/daughter understand the following rules:
• Always keep your profile private
• Never accept friend you do not know in real life
• Never post anything which could reveal your identity including photographs wearing school uniform where possible
• Never post anything you wouldn't want your parents or teachers to see
• Never agree to meet somebody you only know online without telling a trusted adult
• Always tell someone if you feel threatened or someone upsets you
We recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online:
www.thinkuknow.co.uk

www.net-aware.org.uk
www.getsafeonline.org

Through lessons provided at the academy, assemblies, guest speakers, and PSHE lessons, we do our best to provide our children with the awareness and knowledge they need in order to recognise and avoid dangerous, destructive, or unlawful behaviour and to respond appropriately. However, it is only through a collaborative effort between parents and teachers that we will succeed in creating responsible and safe cyber citizens.
If you require any further advice or information, please do not hesitate to contact us at the academy.

Yours faithfully

Appendix 2
Acceptable Use Agreement: Pupils & Parents

Acceptable Use Agreement: Pupils – Primary

Acceptable Use Policy Agreement

Pupil:

The Academy will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. The rules below are set out for my own personal safety as well as others.

Rules for ICT and Internet Use

- I will only access the system with my own username and password.
- I will use the computers for academy work and homework
- I will not bring in any memory sticks or mobile devices from outside the academy
- I will only email people I know, or my teacher has approved
- Any messages I send will be polite and responsible
- I will not disclose or share personal information about myself or others when on-line
- I will be aware of "stranger danger", when I am communicating on-line and will not arrange to meet anyone.
- I will report any unsuitable material or messages sent to me. I understand my report will be confidential and would help protect other children and myself.
- I understand that the academy will check and monitor my computer files and the internet sites I visit.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
- I will not take or send images of anyone without their permission.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the academy community.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, sanctions may apply. This may include loss of access to the school network / internet, suspensions and parents will be contacted.

I have read and understand the above and agree to follow these guidelines.
If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student name:

_____

Student signature: _____ Date: ___/____/_____

Parent/Carer:

Internet and ICT:

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my child access to:

- the internet at school
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. The internet at the Academy is via a filtered and protected system that restricts access to 'safe' internet content.

I understand that the school can, if necessary, check my child's computer files and the internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Social networking and media sites:

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

- I have read and understood the 'rules for ICT and internet use' within the Pupil agreement.
- I understand that if my child(ren) fail(s) to follow the 'rules for internet use' then sanctions may apply. They may have their account suspended and not be allowed to use the internet in future.
- I give permission for my child to use the internet at the academy.

Student's name:

_____

Parent/guardian signature:

_____

Date: ___/____/_____

.Appendix C
Acceptable Use Agreement: Staff

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in the academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Michelle Slymn or Josie Bagley.

- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Principal or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any academy business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in the academy, taken off the academy premises or accessed remotely. Personal data can only be taken out of the academy or accessed remotely when authorised by the Principal or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Josie Bagley
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with the academy policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the academy network without the permission of the parent/ carer, member of staff or Principal
- I will support the academy approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the academy or its community
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available, on request, to my Line Manager or Principal
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in the academy and outside the academy, will not bring the academy, my professional reputation, or that of others, into disrepute
- I will support and promote the academy's Online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the academy between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the academy

Signature …… Date ……

Full Name ……(printed)

Job title ……