Online Safety Policy

Policy Title	Online Safety
Policy Created / Amended	March 2021
Policy Ratified	
Policy review cycle	2 Years
Policy Review Date	March 2023

SAMUEL WARD

SAMUEL WARD

Introduction

As part Keeping Children Safe in Education, it is the duty of the Academy to ensure that children and young people are protected from potential harm both within and beyond the Academy. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.
This policy should be read in conjunction with the Safeguarding Policy, Child Protection Procedures, the Anti-bullying Policy and Staff and persons in a position of trust code of conduct.

Aims

This policy aims:

- To explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.
- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside the Academy.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the Academy.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the Academy

Governors/Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the Academy with further responsibilities as follows:

- The Headteacher has a designated Online Safety Lead and Safeguarding Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the Academy.
- The Headteacher is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed and the Academy's development plan.
- The Headteacher will inform Governors about the progress of, or any updates to, the online safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding.

The Governors MUST ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the Academy. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.

- An online safety Governor (Safeguarding Governor) challenges the Academy about having an AUP (Acceptable Use Policy) with appropriate strategies which define the roles and responsibilities for the management, implementation and safe use of ICT, including:
    - Firewalls - Smoothwall S10

  - Anti-virus and anti-spyware software - **Trend OfficeScan Antivirus**
  - Filters - Smoothwall S10
  - Using an accredited ISP (Internet Service Provider) - **BT Business**
  - Awareness of wireless technology issues
  - A clear policy on using personal devices
  - E-safe internet and computer monitoring software
  -

- Ensure that any misuse or incident has been dealt with appropriately according to policy and procedures, and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via the Academy's agreed protocols with the police) or involving parents/carers.

Local online safety Lead

The online safety lead is the Designated Safeguarding Lead. It is their role to:

- Appreciate the importance of online safety within the Academy and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the Academy.
- Ensure that the AUP is reviewed annually, with up-to-date information and that training is available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-alone PC, staff/children laptops and the learning platform.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher or Behaviour Lead on a regular basis.
- Liaise with the PSHE, safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Transparent monitoring of the Internet and online technologies.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Work alongside the ICT Lead to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
  - Blanket e-mails are discouraged
  - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher.
- Monitor reports of student concerns reported via E-safe and action appropriately, either sanctioning for inappropriate behaviour or implementing safeguarding procedures as appropriate.

Staff or Adults

It is the responsibility of all adults within the Academy to:

- Ensure that they know who the Designated Safeguarding Lead (DSL) is within the Academy so that any

SAMUEL WARD

misuse or incidents can be reported which involve a child.

- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Director of Education must be informed immediately.
- Be familiar with the Behaviour, Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/DSL immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online Safety Lead.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with online safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 2018. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- To ensure that Academy bursars follow the correct procedures for any data required to be taken from the Academy premises.
- Report accidental access to inappropriate materials to the Online Safety Lead and Academy Helpdesk in order that inappropriate sites are added to the list of blocked websites
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the Academy network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted and password protected.
- Report incidents of personally directed 'bullying' or other inappropriate behaviour via the Internet or other technologies using the Academy's standard procedures outlined in the Behaviour Policy.

Children and Young People

Children and young people should be:

- Responsible for following the Acceptable Use Agreement whilst within the Academy as agreed at the beginning of each academic year or whenever a new child attends the Academy for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE, assemblies or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.

Appropriate and Inappropriate Use

By Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the Academy to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. Staff training underpins receipt of this policy.

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the event of inappropriate use: if a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and appropriate authorities contacted. If inappropriate use is detected by the E-safe Monitoring software, this report will be sent directly to the Headteacher.

By Children or Young People

Acceptable Use Agreements and the letter for children, young people and parents/carers are found in the student planner. These detail how children and young people are expected to use the internet and other technologies within the Academy, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The Academy should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the Academy that the agreements are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond the Academy.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and ‘fit for purpose’ based on research for work and be copyright free.

File sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond the Academy.

In the event of inappropriate use: Should a child or young person be found to misuse the online facilities whilst at the Academy, the following consequences will occur:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites to contact friendship groups. No safeguarding issues involved.

Possible Sanctions: ***Referred to Inclusion Officer/Head of Year. Warning may be given, or a lunchtime detention.***

Category B infringements

- 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 (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups. No safeguarding issues.
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it*

Possible Sanctions: ***Referred to Inclusion Officer/Head of Year*** *Removal of Internet access rights for a period / removal of device until end of day / contact with parent.* ****Reported to DSL / online safety coordinator to confirm that material does not pose any safeguarding risks. This could involve the device being given to the police and returned to an adult when and if deemed appropriate. Dependent on content this could lead to more serious sanctions such as fixed term exclusions or permanent exclusion.***

Category C infringements

- Deliberately corrupting or destroying someone’s data; violating privacy of others
- Sending an email or message that is regarded as harassment / bullying *
- Deliberately trying to access offensive or pornographic material*
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions: ***Referred to Inclusion Officer/Head of Year who will immediately notify the Behaviour Lead/DSL/Headteacher as appropriate. DSL to assess any possible safeguarding risks and action appropriately. This could involve the device being given to the police and returned to an adult when and if deemed appropriate. Dependent on content this could lead to more serious sanctions such as fixed term exclusions or permanent exclusion.***

Other safeguarding actions

If inappropriate web material is accessed:

1. Inform the Academy Helpdesk so that the inappropriate website(s) can be added to the blocklist

Category D infringements

- Continued sending of emails or messages regarded as harassment / bullying
- Deliberately accessing, sending, 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 2018
- Bringing the school name into disrepute
- Using texts or images to denigrate pupils or staff

*Possible Sanctions – **Referred to Inclusion Officer/Head of Year who will immediately notify the Behaviour Lead/DSL/Headteacher as appropriate. DSL to assess any possible safeguarding risks and action appropriately. This could involve the device being given to the police and returned to an adult when and if deemed appropriate. Dependent on content this could lead to more serious sanctions such as fixed term exclusions or permanent exclusion..***

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider
3. Ensure any safeguarding issues are also recorded on CPOMS

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

Children are taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

STAFF

Category A infringements (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 - **referred to line manager and Headteacher**. Dependent on material found usually warning given.*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;

- Deliberately accessing, sending, downloading or 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 2018;
- Bringing the school name into disrepute.

*Sanction – **Referred to Headteacher / Governors and follow school disciplinary procedures; in some instances this could lead to referral to LADO (Local Authority Designated Officer). Actions suggested by LADO will be adhered to.***

Other safeguarding actions:

- Remove the device to a secure place to ensure that there is no further access to the device. Device handed over to the police.
- Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Police to identify the precise details of any material that is deemed inappropriate. This is to ensure that members of staff, including the IT department are not put at risk.

If a member of staff commits an exceptionally serious act of gross misconduct they will be instantly suspended whilst investigations are ongoing. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. the Police service to investigate equipment and data evidence as well as the LADO.

Child Pornography

In the case of Child Pornography being found, the member of staff will be **immediately suspended**, the LADO and the Police called. The Academy will support the Police and the LADO with subsequent investigation.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

Appropriate and Inappropriate Use

Internet Use

The Academy teaches pupils how to use the Internet safely and responsibly. They are also taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name/middle name is acceptable)
- Address
- Telephone number
- E-mail address
- School/education setting or other establishment
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from Samuel Ward Academy
- Identifying information e.g. I am number 8 in the Academy's Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people must be stored according to policy.

Pupils with Additional Learning Needs

The Academy strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and Internet access.

Learning Platforms

The uploading of images to the Academy is subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of any images. The Academy will consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

External Websites

In the event that a member of staff finds themselves or another adult on an external website such as 'Rate My Teacher' as a victim, the Academy encourages them to report incidents to the Headteacher using the reporting procedures for monitoring.

E-mail Use

The Academy has e-mail addresses for children and young people to use as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot.

Staff, children and young people use their Academy email address for any communication between home and the Academy only. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with pupils is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of emails where there are communications between home and the Academy on a regular basis. The network manager regularly monitors Internet use and the use of emails. The network manager notifies the appropriate Achievement Director of any infringements.

Mobile Phones and Other Emerging Technologies

Please see Behaviour Policy for our current procedures/policies regarding mobile phone use in school.

Personal Mobile Devices – Students

- Students must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, will be subject to the same procedures as taking images from digital or video cameras
- Students should be aware that games consoles such as Sony Playstation, Microsoft Xbox, Nintendo Wii and other such systems have Internet access which may not include filtering and must not be used in the Academy.
- The Academy is not responsible for any theft, loss or damage of any personal mobile device.
- If a student does bring a mobile phone to school (e.g for personal protection/safety on the way to and from school), whilst on school premises it should be switched off and in a bag or pocket, unless under the direct supervision of staff. Any student seen using a mobile phone on school site will have their phone confiscated for the remainder of the day. Any student seen using their phone on the way out of school but before they have passed the gate will receive a 30 minute after-school detention the following day.

Personal Mobile Devices – Staff

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, will be subject to the same procedures as taking images from digital or video cameras

- Staff should be aware that games consoles such as Sony Playstation, Microsoft Xbox, Nintendo Wii and other such systems have Internet access which may not include filtering and must not be used in the Academy.

- The Academy is not responsible for any theft, loss or damage of any personal mobile device.

Academy Devices

The management of the use of these devices is as follows:

It is policy to ensure that pupils understand the use of a public domain and the consequences of misuse. Relevant curriculum links are made to highlight the legal implications and the involvement of law enforcement. Other technologies which the Academy use with children and young people include:

- Photocopiers
- Fax machines
- Telephones
- Mobile phones
- Cameras
- Video recorders
- Voice recorders
- Tablets

Videos and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in the Academy there is access to cameras, video recorders and voice recorders, this will be monitored by members of staff. Pupils therefore should not have, nor be using, such equipment without the express permission of a member of staff.

The Academy requires that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph, but not both.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

Video-Conferencing / Virtual meetings

Videoconferencing should be via Skype for Business, which is provided via the Office365 platform, or via Microsoft Teams.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the Academy. This process will always be supervised by a member of staff and a record of dates, times and participants held by the Academy.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable UseAgreement.

Managing Social Networking and Other Web 2.0 Technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private place through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Twitter, Snapchat)

In response to this issue the following measures have been put in place:

- The Academy controls access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, Academy name, groups or clubs attended, IM and email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, Academy uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The Academy is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the Academy allowing for the procedures, as set out in the Behaviour Policy, to be followed.

Social Networking Advice for Staff
See also: Unity Schools Partnership Staff Code of Conduct

Social networking outside of work hours, on non-Academy equipment, is the personal choice of all Academy staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.

- Staff should not engage in personal online contact with students outside of systems authorised by the Headteacher (e.g. email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. As such, professional communications using school e-mails and the VLE are permitted. Any abuse of this system should be reported to the relevant member of staff (line manager, any member of SLT (Senior Leadership Team) or Headteacher).

Safeguarding Measures - Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way. Please refer to the Acceptable Use Agreement for Staff and children and young people for the appropriate use of the learning platform.

The BT broadband connectivity has a Smoothwall filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.
All filtering should be set to ‘No Access’ within any setting and then controlled via:

- Group mapping - Existing user groups mapped to Smoothwall policies with a list of blocked or allowed categories

The Academy is responsible for setting its filtering systems and uses a Smoothwall S10 which is managed by the IT Support Team. It is the responsibility of the Governing Body and the Headteacher to ensure that the filtering systems protect young people from inappropriate materials.

The levels listed below are in relation to age appropriate categories:

- IT Staff - Enhanced level of access for IT Support staff to check and access most sites, except core blocked categories such as Adult Content
- Staff- Basic adult policy. This allows for some customisation and the addition of sites if agreed by the IT Network Manager
- Students – Basic student policy. Acceptable website categories are approved by the IT Support Team. Sites designed for older students such as social networking and blogs are blocked, along with core categories
- 6th Form Students - As above, with access to content used for research and collaboration allowed, such as social networking and blog sites
- Internet search engines are forced through ‘safe search’ as a matter of course for all staff and students, with safe search enforced for YouTube for students

The learning platform is set within a filtering service that will provide the same level of protection for all users.

Anti-virus and anti-spyware software (Trend Antivirus and Malware) is used on all network and standalone PCs or laptops and is updated on a regular basis.

SAMUEL WARD

A firewall (Smoothwall S10 series provided by BT) ensures information about people and the Academy cannot be accessed by unauthorised users.

Children should use a search engine that is age appropriate such as Google or Bing with Safe Search enforcement

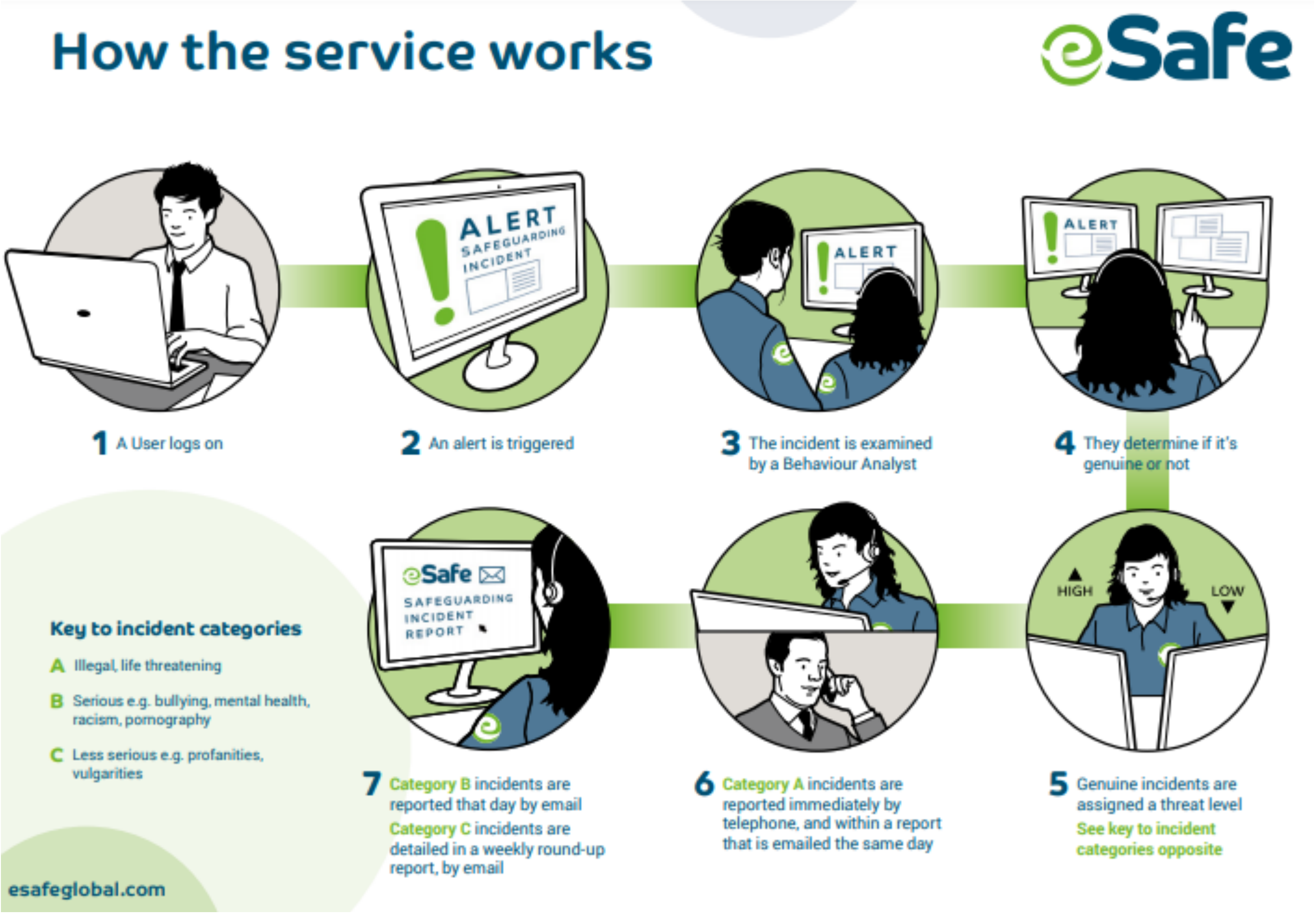
The Report Abuse button is available via the www.thinkuknow.co.uk website should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and Online Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is provided via a tile on the Sharepoint VLE for further advice and information.

E-Safe

The school subscribes to E-safe monitoring for safeguarding staff and students and monitoring the use of school IT equipment, both online and offline, and on site and off site.

If alerts are received (see below), they will be dealt with by the DSL/alternates in respect of students and the Headteacher in respect of staff. Actions for students may include a sanction for inappropriate use of IT, or safeguarding procedures being implemented.



How the service works

1 A User logs on

2 An alert is triggered

3 The incident is examined by a Behaviour Analyst

4 They determine if it's genuine or not

5 Genuine incidents are assigned a threat level
See key to incident categories opposite

6 Category A incidents are reported immediately by telephone, and within a report that is emailed the same day

7 Category B incidents are reported that day by email
Category C incidents are detailed in a weekly round-up report, by email

Key to incident categories

A Illegal, life threatening

B Serious e.g. bullying, mental health, racism, pornography

C Less serious e.g. profanities, vulgarities

esafeglobal.com

Addendum to the staff, pupil and volunteer privacy notices for schools using eSafe

Schools have a statutory duty to monitor their digital environment in order to identify any potential threats to pupil's welfare and wellbeing. At Langer Primary Academy and in our secondary schools (including Churchill and Sir Bobby Robson) this monitoring is carried out by eSafe. eSafe combines intelligent detection software, expert human behaviour analysis and dynamic threat libraries to identify a range of safeguarding risks.

All school owned devices will be continuously monitored for safeguarding risks. If pupils and staff use a school owned device outside of school, the device will continue to be monitored when it is both online and offline.

A Data Protection Impact Assessment (DPIA) has been completed for eSafe. Below is an addendum to the staff, pupil and volunteer privacy notices.

The purposes for processing	To monitor user's activity in the digital environment, provided by the school, in order to detect and alert markers of risk to safety, welfare and wellbeing.
The lawful basis for processing	Schools are legally required to comply with statutory obligations regarding safeguarding and child protection. As such, schools may rely on article 6 (1) (c) of the GDPR (General Data Protection Regulation): processing is necessary for compliance with a legal obligation to which the controller is subject. (The Prevent Duty and the Department for Education's statutory guidance: Keeping Children Safe in Education) And Schedule 1, Part 2, Paragraph 18 of the Data Protection Act 2018, processing special category data for the purpose of safeguarding children and individuals at risk.
The categories of personal data obtained	• User login ID • Date and time stamp of when an incident occurs • ID of the device in use • Screenshot of the user's screen at the moment the incident occurred, details of attempts to access potentially illegal content • Information about a user's health (including mental health such as self-harm/suicide risk) • Information about a user's political opinions where there is a suspicion that those opinions may be extreme or concerning.
The recipients of the personal data	In certain circumstances, when we have a cause for concern, we may share your personal data with police forces, the NHS or local authorities (e.g. social care).
The retention periods for the personal data	eSafe will retain screenshots and reports for six months from the date of an incident. The retention by schools of screenshots and/or reports provided by eSafe for the purpose of investigating concerns is covered in the trust's record retention policy
Your rights	Your rights over your personal data are unaffected and are as stated in the pupil, staff and volunteer privacy notices

Tools for Bypassing Filtering

Web proxies are probably the most popular and successful ways for students to bypass Internet filters today, identifying a cause for concern amongst school/education settings, where children and young people can access the internet. Web proxies also provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content.

A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or information of an adult nature – all of which is blocked through the Academy's filtering system.

Due to the ever evolving nature of this bypassing tool, and the tens of thousands of websites offering set-up guidance, this is not an issue that can be solved overnight. It is referred to within the Acceptable Use Agreement for both staff and pupils as an effective way for the Academy to manage the problem.

SAMUEL WARD

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass the Academy security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

Monitoring

In addition, to E-safe, the Online Safety Lead and Network Manager/ICT technicians are monitoring the use of online technologies by children and young people and staff, on a regular basis.

Teachers should monitor the use of the learning platform and Internet during lessons and also monitor the use of e-mails from the Academy on a regular basis.

Academy Library

The computers in the Academy library and ICT rooms are protected in line with the Academy's network. Where software is used that requires a child login, this is password protected so that the child is only able to access themselves as a user. Children and young people are taught not to share passwords.

The same acceptable use agreement applies for any staff and children and young people using this technology.

Parents – Roles

Each child or young person should receive a copy of the Acceptable Use Agreement on entry to the Academy which needs to be read with the parent/carer, signed and returned to the Academy confirming both an understanding and acceptance of the agreement.

It should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted. The Academy keep a record of the signed forms.

SAMUEL WARD

Curriculum Development

The teaching and learning of online safety is embedded within the Academy's curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line. This is part of the PHSE module but is not exclusive to this area of curriculum and opportunities to embed online safety throughout the curriculum should be sought.

CCTV

To comply with both the Data Protection Act 2018 and the information Commissioner's CCTV Code of Practice, the Academy clearly declares the use of CCTV for security measures in order to inform the public that they are entering a surveillance area and we display the following key information:

- The name of the Academy
- The contact details of who is responsible for the system
- The purpose of the CCTV system

The Academy ensures that all images recorded through the CCTV system are fully traceable with the date, time, recording device and person responsible for recording all detailed in a secure log for audit trail purposes.

SAMUEL WARD