Ocker Hill Academy

e-Safety Policy and Procedure

To be reviewed in line with Ocker Hill Academy Policy Guidelines

Contents:

Statement of intent

Protecting young people and adults properly means thinking beyond the Academy environment. Broadband, Wi-Fi and 3/4G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in the Academy or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an e-Safety Policy demands the involvement of a wide range of interest groups: theTrustees, Principal, SLT, SENCO, DSL, classroom teachers, support staff, parents, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

E-Safety is a child protection issue, and indeed it should not be managed primarily by the ICT Team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying. There is a named

An e-Safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that Ocker Hill Academy will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.
- Within the Academy provide a filtered and monitored online environment for the pupils to safely engage with.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of Ocker Hill Academy community with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the Academy.
- Assist Academy staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other Academy policies.
- Ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

1. Teaching and learning

Why the internet and digital communications are important

1.1. The internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide pupils with quality internet access as part of their learning experience.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behaviour in their use of technology during lessons.

1.5. Teachers remind pupils about their responsibilities through an end-user Pupil Acceptable Use Agreement which every pupil will sign when they log on to the Academy network.

Internet use will enhance learning

1.6. The pupils know that the Academy internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. They will understand that their online experience in the Academy is filtered and monitored and that the filter is set so that their access remains useful.

1.7. All stakeholders will be educated that the filter may not screen out all wanted content and so they will have the skills and responsibility of reporting any instances where content bypasses the filters.

1.8. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.9. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.10. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

1.11. The academy will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.12. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.13. Pupils will be taught how to report unpleasant internet content to the teacher. This can be done anonymously, or in person, and will be treated in confidence.

1.14. Ocker Hill Academy has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files – without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

2. Managing internet access

Information system security

2.1. Academy ICT systems security will be reviewed regularly.

2.2. Virus protection will be updated regularly.

Email

2.3. Pupils may only use approved email accounts on the Academy system.

2.4. Pupils must immediately tell a teacher if they receive an offensive email.

2.5. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

2.6. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.

2.7. The Academy will consider how emails from pupils to external bodies are presented and controlled.

2.8. The forwarding of chain letters is not permitted.

2.9. The Academy:

- Provides staff with an e-mail account for their professional use and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of pupils or staff on the Academy website.
- Will contact the police if one of our staff or pupils receives an e-mail that it considers is particularly disturbing or breaks the law.
- Will ensure that e-mail accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous.

Published content and the academy website

2.10. Staff or pupil personal contact information will not be published. The contact details given online should be the Academy office.

2.11. The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

2.12. Uploading of information is restricted to our website authorisers.

2.13. The Academy website complies with the following statutory DfE guidelines for publications:

- What academies, free schools and colleges should publish online

2.14. Most material is the Academy's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.15. The point of contact on the Ocker Hill Academy website is the Academy address and telephone number. The Academy uses a general email contact address, e.g. office@academyaddress. Home information or individual email identities will not be published.

2.16. Photographs published on the web do not have full names attached.

2.17. The Academy does not use pupils' names when saving images in the file names or in the tags when publishing to the academy website.

2.18. The Academy expects teachers using Academy approved blogs or wikis to password protect them and run from the Academy website.

Publishing pupils' images and work

2.19. Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The Academy will consider using group photographs rather than full-face photos of individual children.

2.20. Pupils' full names will not be used anywhere on the Academy website or other online space, particularly in association with photographs.

2.21. Written permission from parents will be obtained before photographs of pupils are published on the Academy website.

2.22. Work can only be published with the permission of the pupil and parents.

2.23. Pupil image file names will not refer to the pupil by name.

2.24. Parents should be clearly informed of the Academy policy on image taking and publishing, both on academy and independent electronic repositories.

2.25. The Academy gains parental permission for use of digital photographs or video involving their child as part of the Academy agreement form when their child joins the Academy.

2.26. The Academy does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Academy produced video materials/DVDs.

2.27. Staff sign the academy's Staff, Trustee and Visitor Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

2.28. If specific pupil photos (not group photos) are used on the Academy website, in the prospectus or in other high-profile publications, the Academy will obtain individual parental or pupil permission for their long-term use.

2.29. The Academy blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.30. Pupils are taught about how images can be manipulated in their e-safety education programme and to consider how to publish for a wide range of audiences which

might include trustees, parents or younger children as part of their ICT scheme of work.

2.31. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.32. Pupils are taught that they should not post images or videos of others without their permission. The Academy teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or Academy. The Academy teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social networking and personal publishing

2.33. Ocker Hill Academy will control access to social networking sites and consider how to educate pupils in their safe use.

2.34. Newsgroups will be blocked unless a specific use is approved.

2.35. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

2.36. Pupils and parents will be advised that the use of social network spaces outside of the academy brings a range of dangers for primary aged pupils.

2.37. Pupils will be advised to use nicknames and avatars when using social networking sites.

2.38. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.

2.39. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.

2.40. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.

2.41. Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the Academy's preferred system for such communications.

2.42. Academy staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or Academy staff.
- They do not engage in online discussion on personal matters relating to members of the Academy community.
- Personal opinions should not be attributed to the Academy.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

2.43. The Academy's chosen solution for filtering is SENSO Cloud. If staff or pupils come across unsuitable online materials, the site must be reported to the e-Safety Officer/Designated Safeguarding Officer.

2.44. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any violations detected will be triaged by the DSL Team and acted on accordingly.

Managing videoconferencing and webcam use

2.45. Videoconferencing should use the educational broadband network to ensure quality of service and security.

2.46. Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

2.47. Video conferencing and webcam use will be appropriately supervised.

Managing emerging technologies

2.48. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

2.49. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass the Academy filtering systems and present a new route to undesirable material and communications.

2.50. Mobile phones will not be used during Academy time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

2.51. The use by pupils of cameras in mobile phones will be kept under review.

2.52. Staff will not use personal mobile phones to communicate with children or use them to capture images of them. Smart watches worn to the Academy should be used only for the purposes of telling the time or accessing fitness applications.

Protecting personal data

2.53. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

Personal devices and mobile phones

2.54. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the principal. Such authorised use is to be monitored and recorded.

2.55. Ocker Hill Academy reserves the right to search the content of any mobile or handheld devices on the Academy premises where there is a reasonable suspicion

that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

2.56. Where parents or pupils need to contact each other during the Academy day, they should do so only through the Academy's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the Academy office to answer on their behalf or seek specific permissions to use their phone at other than their break times. Mobile phones will not be used during lessons or formal Academy time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

2.57. Mobile phones and personally-owned devices will not be used in any way during lessons or formal Academy time. They should be switched off or on silent at all times.

2.58. Mobile phones and personally-owned mobile devices brought in to the Academy are the responsibility of the device owner. Ocker Hill Academy accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

2.59. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the Academy site, e.g. the classroom.

2.60. The Bluetooth, or similar function, of a mobile phone will be switched off at all times and not be used to send images or files to other mobile phones.

2.61. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned. If images are taken, they should be deleted and the soonest possible instance.

2.62. Staff handheld devices, including mobile phones and personal cameras, must be noted in the Academy – name, make and model, serial number. Any permitted images or files taken in the Academy must be downloaded from the device and deleted in the Academy before the end of the day.

2.63. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

2.64. Staff will be issued with an Academy phone where contact with pupils' parents is required.

2.65. Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods, unless permission has been granted by a member of the SLT in emergency circumstances.

2.66. If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, it will only take place when approved by the SLT.

2.67. Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.

2.68. If a member of staff breaches the Academy policy, disciplinary action may be taken.

2.69. Where staff members are required to use a mobile phone for Academy duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, an Academy mobile phone will be provided and used. In an emergency where a staff member doesn't have access to an Academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

2.70. Pupils will abide by the following rules when using personal devices in the Academy:

- Ocker Hill Academy strongly advises that pupil mobile phones should not be brought into the Academy; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. In such cases, these mobile phones will be kept in a secure place in the classroom until home time and will be switched off..
- If a pupil breaches the Academy policy, the phone or device will be confiscated and will be held in a secure place in the Academy office. Mobile phones and devices will be released to parents in accordance with the Academy policy.
- If a pupil needs to contact their parents, they will be allowed to use an Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupil should bring their mobile phone or personally-owned device into the Academy without consent from a member of staff at the Academy. Any device brought into the Academy without permission will be confiscated. Smart watches worn to the Academy should be used only for the purposes of telling the time or accessing personal fitness applications. If a pupil breaches the Academy policy, the device will be confiscated, stored in a safe place and then released back to the parents.

3. Policy decisions

Authorising internet access

3.1. All staff will read and sign the Staff, Trustee and Visitor Acceptable Use Agreement before using any Academy ICT resource.

3.2. Ocker Hill Academy will maintain a current record of all staff and pupils who are granted access to the Academy ICT systems.

3.3. Any person not directly employed by the Academy will be asked to sign the Staff, Trustee and Visitor Acceptable Use Agreement before being allowed to access the internet from the Academy site.

Assessing risks

3.4. Ocker Hill Academy will take all reasonable precautions to prevent access to inappropriate material through its filtering and monitoring solution and its anti-virus protection; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Academy network. The Academy **cannot** accept liability for any material accessed, or any consequences of internet access.

3.5. The Academy will audit ICT use on a regular basis to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate and effective.

Handling e-safety complaints

3.6. Complaints of internet misuse will be dealt with by a senior member of staff.

3.7. Any complaint about staff misuse must be referred to the Principal.

3.8. Complaints of a child protection nature must be dealt with in accordance with the Academy child protection procedures.

3.9. Pupils and parents will be informed of the complaints procedure (see the Academy's Complaints Policy)

3.10. Pupils and parents will be informed of the consequences for pupils misusing the internet.

3.11. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

Community use of the internet

3.12. Ocker Hill Academy will liaise with local organisations to establish a common approach to e-safety, if necessary.

4. Pupil online safety curriculum

Teaching and learning

4.1. This Academy has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.

- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To know how to narrow down or refine a search.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

4.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

4.3. The Academy will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign.

4.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

4.5. Ocker Hill Academy recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

4.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK

4.7. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the academy child protection procedures.

4.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

4.9. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed around the academy.

4.10. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the academy community will not be tolerated. Full details are set out in the academy's policy on anti-bullying and behaviour.

4.11. There are clear procedures in place to support anyone in the Academy community affected by cyber bullying.

4.12. All incidents of cyber bullying reported to the Academy will be recorded.

Sexual exploitation/sexting

4.13. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

4.14. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

4.15. There are clear procedures in place to support anyone in the Academy community affected by sexting.

4.16. All incidents of sexting reported to the Academy will be recorded.

Radicalisation or extremism

4.17. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

4.18. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

4.19. The Academy understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

4.20. The Academy understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that Academy staff can recognise those vulnerabilities.

4.21. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

4.22. The Academy will monitor its RE curriculum policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

4.23. Senior leaders will raise awareness within the Academy about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

5. Communications policy

Introducing the e - Safety Policy to pupils

5.1. E-Safety rules and guidance posers will be displayed around the Academy building and discussed with pupils regularly. An e-safety display will be kept up-to-date in the Academy building.

5.2. Pupils will be informed that network and internet use will be filtered and monitored with senior staff appropriately following up concerns and violations identified.

5.3. A programme of training in e-safety will be developed by the computing coordinator, PSHE coordinator and DSL.

5.4. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

Staff and the e-safety policy

5.5. All staff will be given the Academy e-Safety Policy and have its importance explained.

5.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

5.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

5.8. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

- Parents' attention will be drawn to the Academy e-Safety Policy on the Academy website.
- The Academy will maintain a list of e-safety resources for parents.
- The Academy will ask all new parents to sign the parent/pupil agreement when they register their child with Ocker Hill Academy.
- The Academy will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

E-safety Activities and Issues

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites	• Pupils should be supervised • Pupils should be directed to specific, approved online materials
Using search engines to access information from a range of websites	• Filtering must be active and checked frequently • Pupils should be supervised • Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with
Exchanging information with other pupils and asking questions of experts via email or blogs	• Pupils should only use approved email accounts to access the Academy internet • Pupils should never give out personal information
Publishing pupils' work on academy and other websites	• Pupil and parental consent should be sought prior to publication • Pupils' full names and other personal information should be omitted • Pupils' work should only be published on moderated sites and only by the Academy administrator.
Publishing images, including photographs of pupils	• Parental consent for publication of photographs should be sought • Photographs should not enable individual pupils to be identified • File names should not refer to the pupil by name • Staff must ensure that published images do not breach copyright laws
Communicating ideas within chat rooms or online forums	• Only chat rooms dedicated to educational use and that are moderated should be used • Access to other social networking sites should be blocked • Pupils should never give out personal information
Audio and video conferencing to gather information and share pupils' work	• Pupils should be supervised • The Academy should only use applications that are managed by approved educational suppliers
Social networking	• Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents • Social networking sites should be blocked on the Academy network • Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online

Useful Resources for Teachers and Parents

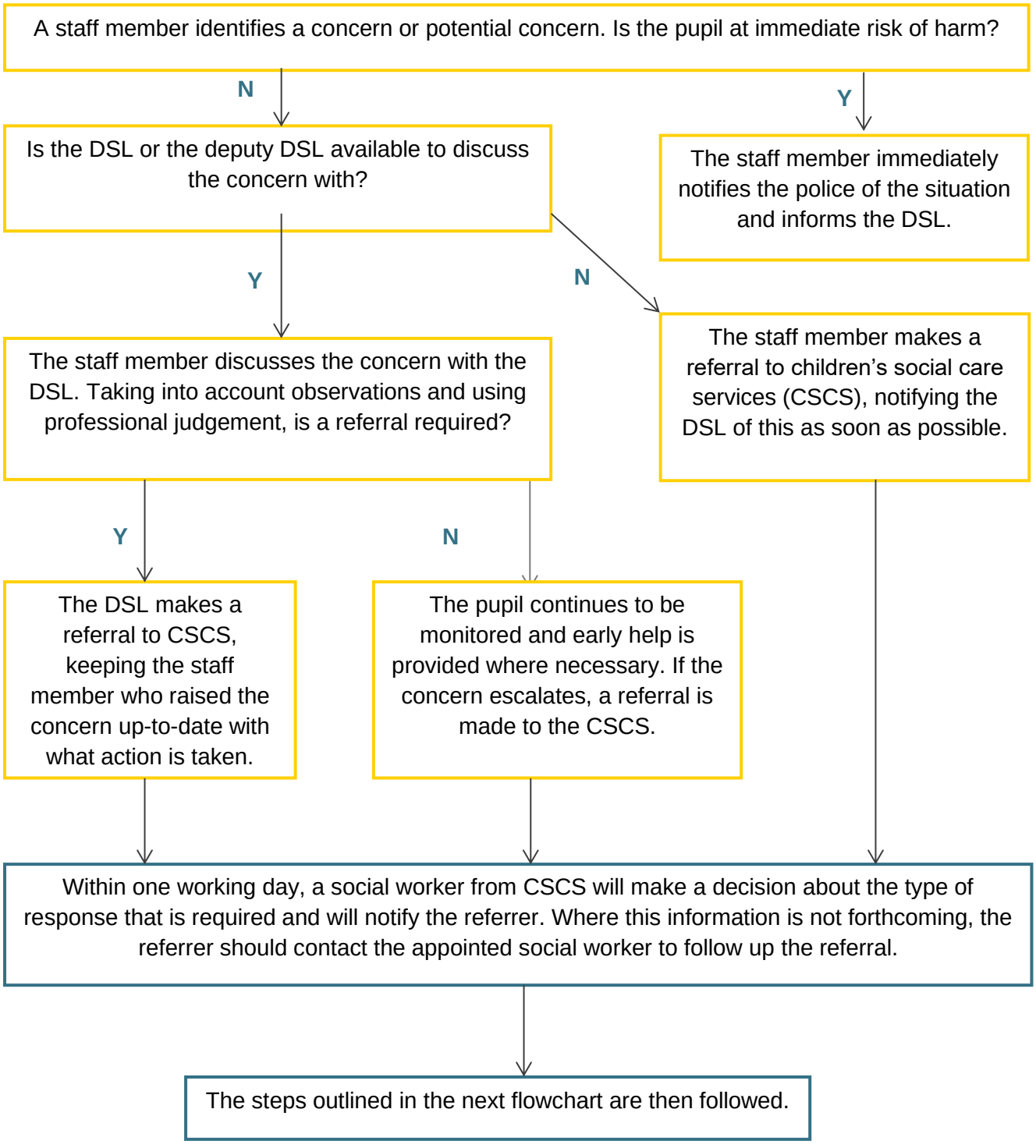
Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school

Response to an Incident of Concern Flowchart

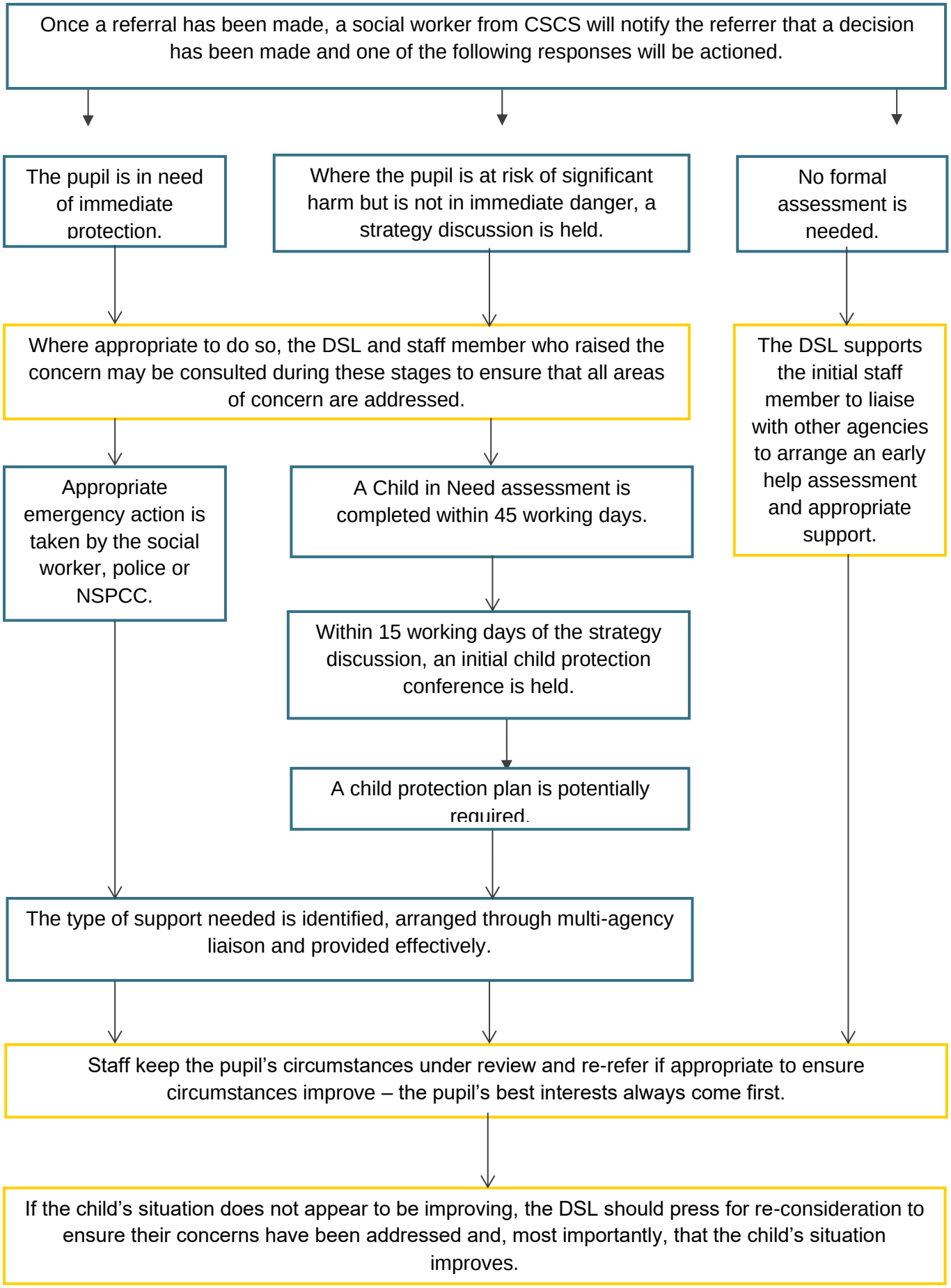
The process outlined within the first section should be followed where a staff member has a safeguarding concern about a child. Where a referral has been made, the process outlined in the 'After a referral is made' section should be followed.

The actions taken by the Academy are outlined in yellow, whereas actions taken by another agency are outlined in blue.

Before a referral is made



After a referral is made



Staff, Trustee and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in the Academy. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, trustees and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the principal**.**

- I will only use the Academy's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the principal.
- 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 personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other Academy-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the academy or accessed remotely when authorised by the Principal and with appropriate levels of security in place.
- I will not install any hardware or software on academy equipment without the permission of the Principal.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- 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 Data Protection Policy and with written consent of the parent or staff member. Images will not be distributed outside the Academy network without the permission of the parent, member of staff or Principal in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Principal.
- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in the Academy and outside, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the Academy's e-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the Academy.

Signature _____

Date _____

Full name _____ (Printed)

Acceptable Use Agreement: Pupils

Class: _____

Year: _____

Pupil Acceptable Use Agreement

- I will only use ICT in the academy for Academy purposes.
- I will only use my own Academy email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the learning platform, Academy network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or academy.
- I will be responsible for my behaviour when using ICT in the academy or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of an academy project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of Academy staff is concerned about my safety.
- I will not bring a mobile phone or other personal ICT device into the academy.

Signature pupil: _____

Signature parent: _____

Date: _____

Rules for KS2

Think then Click

These rules help us to stay safe on the internet

E-safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.