Tapton SCHOOL
Headteacher: Ms Kathryn Rhodes
Tapton School Academy Trust, Darwin Lane, Sheffield, S10 5RG Tel: 0114 267 1414
Email: enquiries@taptonschool.co.uk Web: www.taptonschool.co.uk Twitter: @Taptonschool1

Online Safety Policy

Governor Committee: Full Governing Body

Ratified by Governors: May 2022

Due for review: September 2023

Member of Staff Responsible: Designated Safeguarding Lead

Introduction

At Tapton School, we recognise that the Internet and related communication technologies are essential tools for learning and communication. They can be used in school to enhance the curriculum, challenge students and support creativity and independence. Using ICT to interact socially and share ideas can also benefit our school community. Online safety covers the Internet, but it also covers mobile phones and other electronic communications technologies.

Whilst the online world provides many opportunities, it can also present risks and challenges. These risks include: access to harmful or inappropriate content, data breach, child criminal/sexual exploitation and grooming, copyright infringement, and the potential for excessive use which may impact on the social and emotional development and learning of the student. We also know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings.

Electronic devices and the Internet must be used responsibly and safely by all members of our school community. At Tapton School, we have a duty to ensure that all students, members of staff and parents/carers are protected from potential harm online, whether or not they are using Tapton School's network and devices.

We believe that all students, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse online. We educate students about the risks and responsibilities of online safety and how they should conduct themselves safely. We also appreciate that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential.

Tapton School adopts a whole school approach to Online Safety – we believe it is everyone's responsibility. We aim to work in partnership with students, parents/carers and external agencies to promote students' welfare and help them to be responsible in their approach to online safety.

Aims of the Policy

This policy aims to support with the regulation, management and response to online activity in school and amongst our school community, including students, staff and parents/carers. It should provide readers with a good understanding of appropriate online use.

Members of the school community can use this policy as a reference for their conduct online.

This policy should be read in conjunction with the following policies for further clarity:

• Child Protection and Safeguarding Policy

• Anti-Bullying Policy

• Behaviour Policy

• Staff Code of Conduct (Tapton School Academy Trust)

• Student Acceptable Use Policy (Tapton School Academy Trust)

• Data Protection Policy (Tapton School Academy Trust)

Legal framework

This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in the UK.

Summaries of the key legislation and guidance are available here.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems. This involves the use of the school system both within the school building and remotely.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Tapton School 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 Online Safety.

Issues or conflict that we are made aware of, that has occurred out of school hours, on a student's personal device via their own social media applications, will be addressed in school. We will ensure that parents are informed and in some cases we will inform the police / safeguarding hub, but school sanctions will not necessarily be imposed.

Protecting the Professional Identity of all Staff, Governors and Volunteers

Communication between adults and between students and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

Further details about the conduct of staff with regard to contact with students is contained in the staff Code of Conduct Policy.

Students are expected to adhere to the Acceptable Use Policy, which forms part of the induction to the school. The Acceptable Use Policy is covered in Computer Science lessons, is displayed in the Tapton induction pack and student planners from September 2022.

Breaches of the Acceptable Use Policy are dealt with in line with the School's Behaviour Policy responses can include, but are not limited to, temporary or permanent bans on IT equipment, contact with parents/carers and sanctions such as after school detentions and in serious cases, fixed term suspensions.

Managing Information Systems

Tapton School is responsible for reviewing and managing the security of the computers and internet networks. We take the safeguarding of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats.

Our IT technicians review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted (including safeguarding information which is typically sent via secure sites such as Anycomms)
- Making sure that unapproved software/apps are not downloaded to any school devices. Alerts will be set up to warn users of this.
- Files held on the school network will be regularly checked for viruses

- The use of user logins and passwords to access the school network will be enforced
- For more information on data protection in school please refer to the Tapton School data protection policy. This can be found on the website.

Smoothwall Monitoring and Filtering

Tapton School uses appropriate systems to filter and monitor internet use on all school owned or provided internet enabled devices (both in school and when used remotely). The system applied to do this is called Smoothwall and it covers both staff and student online use. The purpose of Smoothwall systems is to limit online risks and ensure that online usage remains safe and appropriate at all times.

Internet and online use is carefully monitored through individual staff and student log-ins. The Smoothwall filtering and monitoring system will report on all searches, clicks and typing that appears inappropriate. It also blocks sites which can be categorised as: adult content (pornography), criminal activity, racial hatred, radicalisation and extremism, suicide and bullying.

Any concerns identified via monitoring approaches will be reported to the Safeguarding Team, who will respond in line with the Safeguarding and Child Protection Policy and its procedures for dealing with allegations against members of staff.

All users (including staff and students) have been informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils and that effective classroom management and regular education about safe and responsible use is essential.

Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: South Yorkshire Police, The Internet Watch Foundation (IWF) or The Child Exploitation and Online Protection (CEOP).

Cloud Storage

Students and staff have access to Office 365 and One Drive (an online cloud storage resource), both in school and at home via an internet connection. Students and staff must use it in a sensible manner, or they may have access restricted. Students and staff must be aware of and agree to the following:

- They will not type any form of libel, slander, profane or inappropriate, rude or suggestive language in any posts/newsfeed.
- They will not upload any materials that could potentially harm the school network or that could be used for inappropriate use, remembering that it is for educational purposes.
- They understand that the Office365 account and use of the system is monitored at all times.

If any user violates any of these provisions, their access to the network may be terminated and all future access could possibly be denied and other appropriate actions may be taken.

Tapton School has clear guidelines regarding the use of cloud storage/cloud computing which ensures that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data at all times, 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.
- Transfer data using encryption and secure password protected devices.

Data Protection and Other Legislation

Tapton School believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress.

The school collects personal data from students, parents/carers and staff and processes it to support teaching and learning, monitor and report on student and teacher progress and strengthen our support provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents/carers fully informed of the how data is collected, what is collected, and how it is used. GCSE and AS results, attendance and registration records, special educational needs data and any relevant medical information are examples of the type of data that the school needs.

Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulation 2018, and following principles of good practice when processing data, Tapton School will:

- Ensure that data is fairly and lawfully processed.
- Process data only for limited purposes.
- Ensure that all data processed is adequate, relevant and not excessive.
- Ensure that data processed is accurate.
- Not keep data longer than is necessary.
- Process the data in accordance with the data subject's rights.
- Ensure that data is secure.
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where Tapton School is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example, our local authority, Ofsted, or the Department of Health. These authorities are abreast of current data protection law and have their own policies relating to the protection of any data that they receive or collect.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

For more information on the school's safeguards relating to data protection read the Data Protection Policy.

Communication

The school uses email internally for staff and students, and externally for contacting parents/carers and external agencies. It is an essential part of our school communication. Staff and students should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents/carers, students, other members of staff and other professionals for work purposes. This is important for confidentiality. Tapton School has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Appropriate use for students is included in our Acceptable Use Policy (Appendix B) and for staff please see the Staff Code of Conduct.

Guidance for Members of Staff

- Staff should only use official school-provided email accounts to communicate with students, parents/ carers and external agencies. Personal email addresses, text messaging or social media must not be used for these communications at any time.
- Any digital communication between staff and students or parents/carers (email, chat, Office365 etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Whole class/group email addresses may be used by members of staff. Students will be provided with individual school email addresses for educational use.
- Staff MUST NOT use their own phone for school business. They will use the school systems or school provided mobile phones so that calls, messages etc are open and can be monitored to ensure the safety of all students and staff.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the Staff Code of Conduct.

Guidance for Students

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the Computer Science curriculum and in any instance where email is being used within the curriculum or in class:

- In school, students should only use school-approved email accounts.
- Excessive social emailing will be restricted.
- Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Students must be careful not to reveal any personal information over email.

Students will be educated to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Policy and Guidance of Safe use of Student's Photographs and Work

At Tapton School, we want to celebrate the achievements of our students and therefore we may wish to use images and videos of our students or their schoolwork within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. Tapton School does however recognise the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation 2018, images of students and staff will not be displayed in public, either in print or online, without consent. On admission to Tapton School, parents/carers will be asked to sign a photography consent form, which covers the time when the students are a member of the school community.

This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used.
- How long parents are consenting the use of the images for.

- School policy on the storage and deletion of photographs. Only images created by or for the school will be used in public and students may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children.
- Parents/carers and others attending events can take photographs and videos of those events for domestic purposes. For example, parents/carers can take video recordings of a school performance involving their child.
- Tapton School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the school to prevent.
- Tapton School asks that parents/carers and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

We will seek the consent of students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

For more information on please refer to the Data Protection Policy.

Appropriate Use of Photo/Video

Staff and students should be aware that images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Staff/students should know how to protect themselves from this:

- Take care and know the risks when using digital images and 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 school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student and parents or carers
- Staff must check Bromcom photo permissions before posting / using images.

The 4 Cs

There are four ways in which students can be harmed online. In Keeping Children Safe in Education 2021, this is summarised as the 4 Cs:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: child on child abuse or pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and cyber bullying / child on child online abuse.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

To address the risks above, we aim to educate students about online safety as part of our curriculum. For example, the safe use of social media; the internet and technology; Keeping personal information private; How to recognise unacceptable behaviour online; How to report any incidents of cyber-bullying, ensuring students are encouraged to do so, including where they are a witness rather than a victim.

We also aim to educate parents/carers about online safety via our website and via communications sent directly to them via MCAS. We share clear procedures with parents/carers so they know how to raise concerns about online safety.

Members of the Inclusion Team are also engaged regularly in speaking to students and families about the 4 Cs. In cases where online safety is a concern, they will support students and discuss with them the related risks and responsibilities**.** The Inclusion team may also support students in reporting offensive online content and conduct via CEOP/ South Yorkshire Police. Referrals to external agencies such as Social Care and CYT made also be made whereby online safety is a significant concern.

Social Networking, Social Media and Personal Publishing

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online.

Students are taught through the Computer Science, Personal Development curriculum and assemblies. We regularly share information with parents and carers via MCAS and with students via their school email accounts about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

Tapton School follows these general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways.
- Any sites that are to be used in class will be risk-assessed by the teacher prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

If a student is concerned about another person's conduct, content or contact on social media or on any online platform, they should feel able to speak to a member of staff about this, for example, their Form Tutor, Year Leader or any member of the Inclusion Team. We will always reassure students and act if necessary. This action may include removal from school internet access, parents being informed, referrals to external agencies or in the most serious cases to Safeguarding Hub or the police.

Social Media - Protecting Professional Identity

School staff should ensure that:

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

- Security settings on personal social media profiles are regularly checked and upheld to minimise risk of personal information being compromised.

The school's use of social media for professional purposes will be checked regularly to ensure compliance with Data Protection and Communications Policies.

Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use should be appropriate and responsible at all times.

Some issues surrounding the possession of these devices are that they:

- Can make students and staff more vulnerable to cyberbullying.
- Can be used to access inappropriate internet material.
- Can be a distraction in the classroom.
- Are valuable items that could be stolen, damaged, or lost.
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Students who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone or electronic device may be confiscated.

At Tapton School, mobile phones, iPods and other electronic devices such as wireless earphones are not allowed to be visible in the school building during our working hours – 9.10-3.30 – this is non-negotiable. This includes all areas of the Dining Room. If students choose to bring devices to school, they must be put them away before entry into the building so they are not at all visible – this includes earphone cables hanging out of shirts and from pockets, headphones worn around necks and phones in hands.

From the 9.10 bell any such items will be confiscated without discussion. If a student refuses to hand over the item on call will be used. The attending team will confiscate the item and inform the student of the same day After School Detention for defiance. Failure to hand over a confiscated item will result in a fixed term suspension.

The first time an item is confiscated it will be held in the school office until the end of the school day.

If a student has an item confiscated for a second time the parents and carers must come into school to collect the item and to meet with the Year Leader, SLT link or Deputy Headteacher to discuss their child's refusal to comply with our rules. All subsequent confiscations will then also go into the safe awaiting a parent/carer meeting.

These rules around confiscations apply to all students Years 7-13 (and any Year 14 students).

The following points should also be noted with regards to students' use of phones and electronic devices:

- Tapton School will not tolerate cyber bullying against either students or staff. Incidents of cyber bullying will be dealt with seriously, in accordance with the school's Behaviour and Anti-Bullying Policy.
- Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions, please see the school's Behaviour Policy and Anti-Bullying Policy.
- A member of staff can confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Students are not allowed to have mobile phones or personal devices on their possession in examination rooms, they must be handed in to the invigilator. Students are reminded of this at the start of every

exam. If a student is found with a mobile phone/device in their possession, even if switched off, it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being disqualified. If a student fails to hand in their phone/device and instead leaves it in their coat pocket/bag and it sounds during an exam, this would disturb other students so would also be reported to the examining body as malpractice.

-

Unsuitable / Inappropriate Online Activities

We understand that young people are increasingly using electronic equipment on a daily basis to access the internet and share content and images via social networking sites such as Facebook, TikTok, Snapchat and Instagram. Unfortunately, some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings.

Students may also be distressed or harmed by accessing/ being exposed to inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Some internet activity, for example accessing child abuse images or distributing racist material is illegal and is therefore banned from school and all other technical systems. Instances of this would be dealt with very seriously. permanent exclusion, parents/carers would be contacted and sanctions would be applied for the students involved. Such incidents would also result in referrals being made to external agencies such as the Police and Social Care via the Sheffield Safeguarding Hub.

While it is legal, other online misuse, for example cyber bullying is also considered unacceptable at Tapton School. It is also a breach of the school's behaviour policy and in these cases, students may receive sanctions and parents/carers would be contacted. In some cases, referrals to external agencies may be made for additional support, such as the Police or Social Care.

Responding to Incidents of Online Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Please read page 10 of this policy and refer to Appendix A for full details of how Tapton School aims to manage and respond to incidents of online misuse.

If any reported misuse appears to involve illegal activity including (but not limited to):

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Criminal conduct, activity or materials.

The DSL should be consulted, with a view to reporting the incident to the Police and to preserve evidence.

It is intended that incidents of online misuse will be dealt with through normal behaviour / disciplinary procedures for students.

Cyberbullying

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. Tapton School, as with any other form of bullying, takes cyber bullying, very seriously. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Information about the school's management and response to prevent and tackle bullying is set out in the Anti-Bullying Policy and Behaviour Policy.

If an allegation of cyber bullying / child on child online abuse does arise, Tapton School will:

- Take this matter seriously
- Act as quickly as possible to establish the facts. This may involve conducting a formal investigation, which will be led by members of the Inclusion Team and supported by members of the Senior Leadership Team. It may be necessary to take written accounts from the students involved and to examine school systems and logs or contact the service provider to identify the full details of the incident.
- Record the incident appropriately, on Bromcom/ CPOMS depending on the severity of the incident.
- Provide support and reassurance to the victim/s.
- Take the relevant action to sanction the perpetrator/s in accordance with the school's behaviour policy and to contact the parents/carers of those involved.
- It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

Sexting and the Consensual / Non-Consensual Sharing of Nude and Semi-Nude Images of Children.

All incidents involving sexting and the sharing of nude and semi-nude images of children (regardless of whether this is consensual or not) should be responded to in line with the school's Safeguarding and Child Protection Policy.

When an incident involving sexting and/or the consensual/non-consensual sharing of nude and semi-nude images of a child comes to the attention of Tapton school:

- Members of staff will refer the incident to the DSL/DDSL as soon as possible. This should be done by logging the incident on CPOMS and speaking with the DSL/DDSL immediately.
- The Safeguarding team will speak with the student/s involved and contact parents/carers. We may seize the phone/electronic device if it is believed to contain nude or semi-nude images.
- A referral will usually be made to the Police and Social Care via the Sheffield Safeguarding Hub.
- The seized phone will be handed to either parents/carers or to the Police. Parents/Carers are encouraged to delete inappropriate content.
- All information will be recorded accurately on CPOMS.

Members of staff must NEVER attempt to view, share or delete the image or ask anyone else to do so. If a member of staff is shown an image by mistake, they must inform the DSL/DDSL of this.

It is important that everyone understands that whilst sexting and the sharing of nude/ semi-nude images is illegal, students are encouraged to come and talk to members of staff if they have made a mistake, encountered a problem in this area or know someone who has.

Illegal Incidents

If a suspicion or concern is raised that suggests students or members of staff have accessed/ been exposed to a website/online platform that may contain child abuse images, or if there is any other suspected illegal activity, Tapton school will take serious action including permanent exclusion/ disciplinary action for staff.

If the concern relates to a student or group of students, members of staff should log this on CPOMS immediately and speak with a member of the Safeguarding Team, who are listed below:

Kath Tabani (Designated Safeguarding Lead)

Esther Jackson (Deputy DSL)

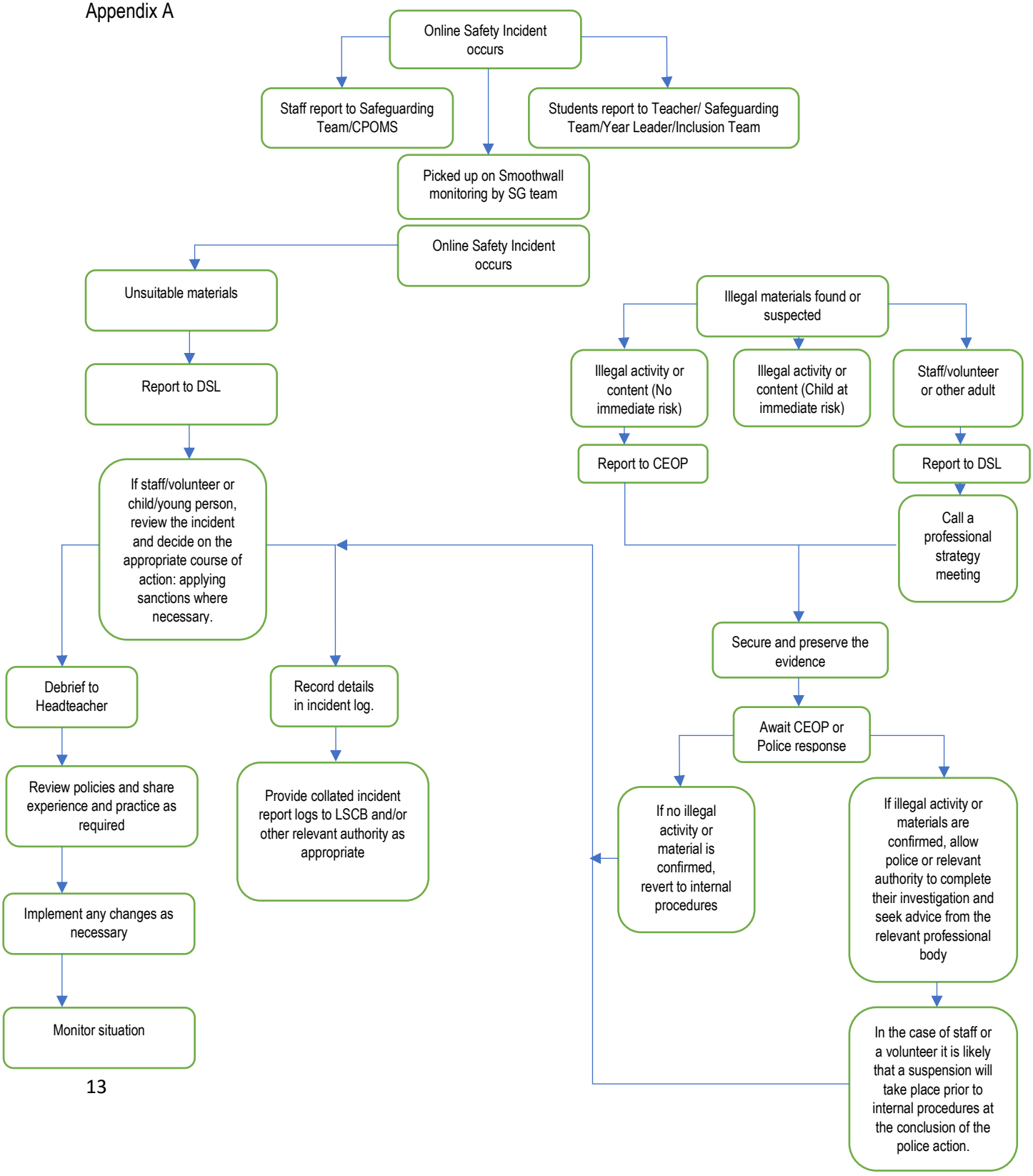
Munna Mohammed (Safeguarding Assistant)

Incidents may be reported to the Police and/or Social Care via the Sheffield Safeguarding Hub for additional support.

If the concerns relate to a staff member's online activity, this should be reported directly to Kat Rhodes, Headteacher. The incident may be reported to the police.

Further details of the actions taken with regards to online safety incidents are listed in the flowchart in Appendix A.

Appendix A


Online Safety Incident occurs
Staff report to Safeguarding Team/CPOMS
Students report to Teacher/ Safeguarding Team/Year Leader/Inclusion Team
Picked up on Smoothwall monitoring by SG team
Online Safety Incident occurs
Unsuitable materials
Report to DSL
If staff/volunteer or child/young person, review the incident and decide on the appropriate course of action: applying sanctions where necessary.
Debrief to Headteacher
Review policies and share experience and practice as required
Implement any changes as necessary
Monitor situation
Record details in incident log.
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials found or suspected
Illegal activity or content (No immediate risk)
Illegal activity or content (Child at immediate risk)
Staff/volunteer or other adult
Report to CEOP
Report to DSL
Call a professional strategy meeting
Secure and preserve the evidence
Await CEOP or Police response
If no illegal activity or material is confirmed, revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of staff or a volunteer it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action.

Appendix B – Acceptable user policy

Appendix C Useful links

CEOP https://www.ceop.police.uk/Safety-Centre/

Sheffield Children's Safeguarding Partnership https://sheffieldscb.proceduresonline.com/p_online.html

UK Safer Internet Centre https://saferinternet.org.uk/professionals-online-safety-helpline

Childnet https://www.childnet.com/

NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/

SWGfL https://swgfl.org.uk/

Digital Parenting https://www.vodafone.co.uk/mobile/digital-parenting

Internet Matters https://www.internetmatters.org/

Parentzone https://parentzone.org.uk/

CBBC https://www.bbc.co.uk/bitesize/guides/z9p9kqt/revision/1

Gov.uk Teaching online safety in schools https://www.gov.uk/government/publications/teaching-online-safety-in-schools