Clapton Girls' Academy
Est. 1906

Policy No: 26
Online Safety Policy and
Acceptable Use Agreement for Students

Clapton Girls' Academy is committed to safeguarding and promoting the wellbeing of young people and expects all staff and volunteers to share this commitment.

Online Safety Policy and Acceptable Use Agreement for Students

Coordinator	Dominic Fyles
Review Frequency	Annually
Policy First Issued	March 2013
Last Reviewed	May 2023
Date policy considered by External HR Consultant	N/A
Date policy considered by External Solicitor	N/A
Agreed by LT on	23rd May 2023
Does this policy need to be agreed by Trustees? **If yes, which committee?**	No N/A
Agreed by Trustees on	N/A
This policy is communicated by the following means:	
Trustees	Trustee consultation by e-mail when policy reviewed and agreed
Staff	Policy folders on staff SharePoint
Parents	Academy website
Students	In IT and Computing lessons, student planners, student leadership groups

Contents

1. Overview

Information and Communications Technology (ICT) plays a significant role in the daily life of students and is an essential resource to support curriculum development, teaching, learning and assessment. At Clapton Girls' Academy (CGA) we build the use of ICT into our curriculum to equip our students with the skills they will need to access life-long learning and employment.

At CGA, the purpose of internet use in is to raise educational standards, promote student achievement, support the professional work of staff and to enhance our management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is, therefore, an entitlement for students who show a responsible and mature approach to its use. We have a duty to provide students with quality internet access. Students use the internet outside of the academy and need to learn how to evaluate internet information and to take care of their own safety and security.

This Online Safety Policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet technologies provided by the academy as well as technologies owned by students.

All references to parents in this policy refers to parents and adults that have parental responsibility.

2. Policy Aim

We aim to educate our students about the benefits and risks of using technology and, therefore this policy provides safeguarding awareness for users to enable them to safely control their online experiences.

In addition, this online safety policy will operate in conjunction with other policies including:

- Behaviour for Learning (Policy 34)
- Challenging Bullying (Policy 28)
- Curriculum, Quality of Teaching, Learning and Assessment (Policy 1)
- Email and Internet Usage Policy and Guidelines for Staff (Policy 55)
- Child Protection Safeguarding Children and Promoting Welfare (Policy 14)
- Staff Code of Conduct (Policy 17)
- Mobile Phone (Policy 61)
- Site and Cyber Security Policy (Policy 59)

This policy is part of the academy's statutory safeguarding policy and applies to all members of the academy's community (staff, students, volunteers, parents, visitors), who have access to the ICT systems. Any issues and concerns relating to online safety must be addressed by referring to the academy's safeguarding and child protection processes.

3. Main areas of risk

Content:

- exposure to illegal, inappropriate or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language)
- lifestyle content , for example pro-anorexia/self-harm/suicide sites or on social media platforms
- hate sites and extremist content
- content validation: how to check authenticity and accuracy of online content

Contact:

- being subjected to harmful online interaction with other users
- grooming
- child sexual exploitation
- cyber-bullying in all forms
- extremism and radicalisation
- identity theft and sharing passwords

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (socialising, watching video or gaming))
- sending and receiving of personally intimate images, also referred to as Youth Produced Sexual Imagery (if self-produced) or Child Abuse Imagery (if not self-produced)
- copyright (no thought or consideration for individual property and ownership – such as music and film)

The academy Online Safety Co-ordinator (Mr Fyles as Designated Safeguarding Lead) works closely with the Head of Computing and ICT and the ICT Network Manager to lead on online safety. Together they work in an Online Safety group with other stakeholders.

4. Roles and Responsibilities

4.1 The Headteacher

The Headteacher must:

- Be adequately trained in off-line and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.
- Lead a 'safeguarding' culture, ensuring that online safety is fully integrated with academy-wide safeguarding.

- Be the Senior Information Risk Owner (SIRO) and take overall responsibility for data management and information security ensuring that academy provision follows best practice in information handling or delegate this responsibility to the Academy Business Leader.
- Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of students, including students at risk of being radicalised or groomed.
- Ensure that there are systems in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager.
- Receive regular feedback from the Online Safety Co-ordinator.
- Ensure Trustees receive regular updates on the nature and effectiveness of the academy's arrangements for online safety.
- Ensure the academy website includes relevant information which is accurate and appropriate.
- Take overall responsibility for online safety provision.

4.2 Trustees , including the safeguarding trustee

- Ensures that the academy has in place policies and practices to keep students and staff safe online
- Supports the academy in encouraging parents and the wider community to engage in online safety activities

4.3 The Online Safety Co-ordinator

Works in conjunction with the Head of Computing and ICT to carry out the following duties:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy's online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Facilitates training and advice for staff..
- Liaises with academy ICT support team.
- Receives reports of online safety incidents and uses these to inform future online safety developments.
- Reports to the leadership team on online safety matters.
- Receives regular updates and/or training in online safety issues and legislation and is aware of the potential for serious child protection concerns. Uses 'Teaching Online Safety in school 2019' to ensure that students ICT curriculum includes how to stay safe and behave online.
- Ensures an annual online safety audit takes place.
- Monitors student internet use through NetSupport DNA and acts accordingly when alerted to any inappropriate usage.
- Updates the academy website and Twitter with online safety information.

- Organises an annual online safety session for parents.
- Uses planned activities to share awareness of online safety issues during Safer Internet Day to support teaching about being safe online.
- Liaises with marketing team to address inappropriate content on academy site, or academy social media pages.
- Supports the reporting of inappropriate content on social media platforms regarding students, staff or the academy to the platform's parent company.

4.4 Students

All students in the academy:

- Read, understand, sign and agree to adhere to the Online Safety and Acceptable Use Agreement for students, found in students' planners, in order to have access to the internet at CGA and use any technological devices. (See appendix 1)
- By signing this agreement, students agree to follow the rules of internet usage and online safety at CGA. Posters (Your internet- Staying safe online) around computers and the academy reinforce this agreement. (See appendix 2).
- Agree to read and use the Microsoft Teams Basic User Guide (for Windows) when attending remote lessons or assemblies. (See appendix 5a).
- Are responsible for using the academy's ICT systems in accordance with this policy
- Should know and understand academy policies on the taking/use of images and cyber-bullying.
- Need to understand the importance of reporting abuse and misuse, access to, inappropriate materials and know how to do so.
- Will be expected to know, understand and follow the academy policies on the use of mobile phones, digital cameras and hand-held electronic devices.
- Have a good understanding of research skills and the need to avoid plagiarism.
- Should understand the importance of adopting good online safety practice when using digital technologies outside the academy and realise that the academy's online safety policy covers their actions out of academy hours, if related to their membership of the academy.
- Must report any unsuitable sites, or concerning social media content, they discover. The URL (address), time and the content must be reported to a member of staff onsite and to a parent/carer, when using the internet outside of the academy.
- Should be aware that their internet use will be monitored and removed if there is serious abuse of this privilege.

4.5 Parents

Parents will be responsible for:

- Reading and promoting the academy's Online Safety and Acceptable Use Agreement for students with their child.

- Endorsing the Parents' Acceptable Use Agreement, which includes reference to their child's use of the internet.
- Playing an active role in monitoring their child's use of the internet outside of the academy
- Reinforcing and supporting the academy's messages about staying safe online.
- Attending the annual online safety session and parent information meetings where online safety advice is shared.
- Appendix 3 refers to how parents can protect their children on their smartphone. This appendix is part of the Mobile Phone policy 61.

4.6 Staff

Staff have a responsibility to:

- Embed online safety in the curriculum.
- Create a culture that incorporates the principles of online safety across all elements of academy life.
- Ensure that they are always vigilant when supervising or teaching with the use of IT, which includes taking an 'it could happen here' approach to online safety issues.
- Use the NetSupport DNA Teacher app when necessary to monitor student activity to avoid any potential online safety breaches.
- Embed understanding of good research skills, the need to avoid plagiarism and keeping up to date with copyright regulations in the curriculum.
- Supervise and guide students carefully when engaged in learning activities involving online technology (including extra-curricular and extended academy activities if relevant)
- Report any student misuse of ICT to the Online Safety Co-Ordinator.
- Report online safety issues (reported by students) to the Online Safety Co-Ordinator or ICT Network Manager via email or the appropriate reporting system.
- Complete all provided training relating to online safety principles, including GDPR related updates.

There is a separate policy that covers staff online safety (see policy no 55 Email and Internet Usage Policy and Guidelines for staff.) This document must be read by all staff.

4.7 Head of Computing and ICT

Works in conjunction with the online safety co-ordinator to oversee the following duties:

- Support the Online Safety Co-ordinator in the review of the academy's online safety policies / documents.
- Takes day to day responsibility for online safety issues that arise within the Computing and ICT department.
- Ensures that all Computing and ICT staff follow the correct procedure in the event of an online safety incident taking place.

- Facilitate initial training of Net Support DNA teacher app for new Computing and ICT staff.
- Liaises with academy ICT support team. in order to ensure correct working of safeguarding infrastructure and advice on site-based safeguarding processes
- Uses 'Teaching Online Safety in school 2019' to ensure that students Computing and ICT curriculum includes how to stay safe and behave online.
- Supporting Computing and ICT teachers to monitors student internet use through NetSupport DNA teacher app and acts accordingly when alerted to any inappropriate usage.
- Make recommendations for updates the academy website and Twitter with online safety information.
- Participate in creating resources for online safety sessions for parents.
- Oversees the creation, and delivery of, activities to share awareness of online safety issues during Safer Internet Day, through KS3 ICT lessons.

4.8 ICT Network Manager/ICT Technicians

Have the responsibility to:

- Monitor and report online safety related issues that come to their attention to the Online Safety Co-ordinator/Headteacher.
- Manage the academy's computer systems, ensuring:
  - the academy password policy is strictly adhered to
  - monitoring systems are in place for misuse detection and malicious attack and are kept up to date (e.g. keeping virus protection up to date)
  - access controls/encryption exist to protect personal and sensitive information held on academy-owned devices
  - the academy's application of web filtering is applied and updated on a regular basis
- Keep up to date with the academy's online safety policy and technical information and inform and update others as relevant.
- Regularly monitor the use of academy technology and online platforms and report any misuse or attempted misuse to the Online Safety Co-Ordinator.
- Ensure appropriate backup procedures and disaster recovery plans are in place
- Keep up-to-date documentation of the academy's online security and technical procedures.

5. Unacceptable Use and Network Security

This section covers the use of academy hardware, including computers, laptops, Chromebooks and iPads. The following policies: (34) Behaviour for Learning, (06) Uniform and (61) Mobile Phone policies make it clear that at no point during the academy day should students in Years 7-11 be accessing the internet using mobile phones as these should be switched off and placed securely in bags or lockers. Mobile phones are banned while students are on the academy. "Banned" means that they must be always switched off and completely out of sight between entering and leaving the academy site.

As part of their induction on using mobile devices, all students including those in Years 12 and 13, sign the Online Safety and Acceptable Use Agreement for students and there are *Guidelines for Acceptable use of Devices* to remind them about this.

Examples of unacceptable use include, but are not limited to:

- Logging in with another person's user ID and password, or using a machine left unattended, but logged in by another user, without permission of the user.
- Creating, transmitting, displaying or publishing any material (text, images or sounds) that are likely to harass, cause offence, inconvenience or needless anxiety to any other person.
- Unauthorised accessing of data and resources on the academy's network system that belong to other "users".
- Taking action that would cause:
    - Corruption or destruction of other users' data.
    - Violation of the privacy or dignity of other users.
    - Intentional waste of time or resources on the academy's network or elsewhere.

If a student discovers a security problem, for example being able to access other users' data, they must inform a member of staff immediately and not show it to other users. Students will be sanctioned if they have been identified as a security risk or have misused ICT facilities.

Possible sanctions include:

- meeting an ESA, teacher , Head of Year, the Online Safety Co-ordinator or the Headteacher;
- informing parents;
- removal of internet or computer access for a period;
- referral to Local Authority, Children's Social Care and/or police.
- internal exclusion or suspension , depending on severity of misuse.

The Online Safety Co-ordinator acts as first point of contact for any misuse. Any concern about staff misuse must be referred to the Headteacher.

Network security is maintained in the following ways:

- The academy uses a hosted firewall with the broadband provider RM called Fortigate 3000D, Version:7.0.5 and is centrally hosted on RM infrastructure to keep our network safe and secure from external threats
- Using Windows Defender Security Centre / System Centre Endpoint Protection on all PCs to secure them from all type of viruses.
- RM SafetyNet and NetSupport DNA is being used to block all the inappropriate website access for the whole school.

- Ublock origin is installed through group policy to protect from unwanted threats generated by ads on browsers.
- Email security is configured as per the NCSC (National cyber security centre) guidelines and protects our email domain from spoofed attacks.

6. Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices are brought into the academy, entirely at the students, staff members', parents' or visitors' own risk. The academy accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into the academy.
- The recording, taking and sharing of images, video and audio on any personal mobile device is prohibited, except where it has been explicitly agreed by the Headteacher. Such authorised use will be verified by the Headteacher (verbally or in writing).
- All mobile device use is to be open to monitoring scrutiny and the Headteacher can withdraw or restrict authorisation for use at any time, if deemed necessary.
- Mobile phones and electronic devices must not be taken into examinations. Where a device (laptop or reading pen) is needed as part of a student's access arrangements, staff will be guided by the Exams Officer to ensure examination protocol is adhered to.
- Sixth form students can only use mobile phones in the Zone, other designated 6th form study areas (e.g. dining pavilion study session and upstairs in the Nightingale building) or when their teacher has given students permission to use mobile phones in a lesson for teaching and learning purposes. For example, to use the Kahoot app.
- Appendix 3 refers to how parents can protect their children on their smartphone. This appendix is part of the Mobile Phone policy 61.

7. Digital images and videos

At CGA, we gain parental permission for use of digital photographs or video involving students as part of the admissions process when students join the academy. Permission is not required for the one image of a student on SIMS, which is there for safeguarding purposes.

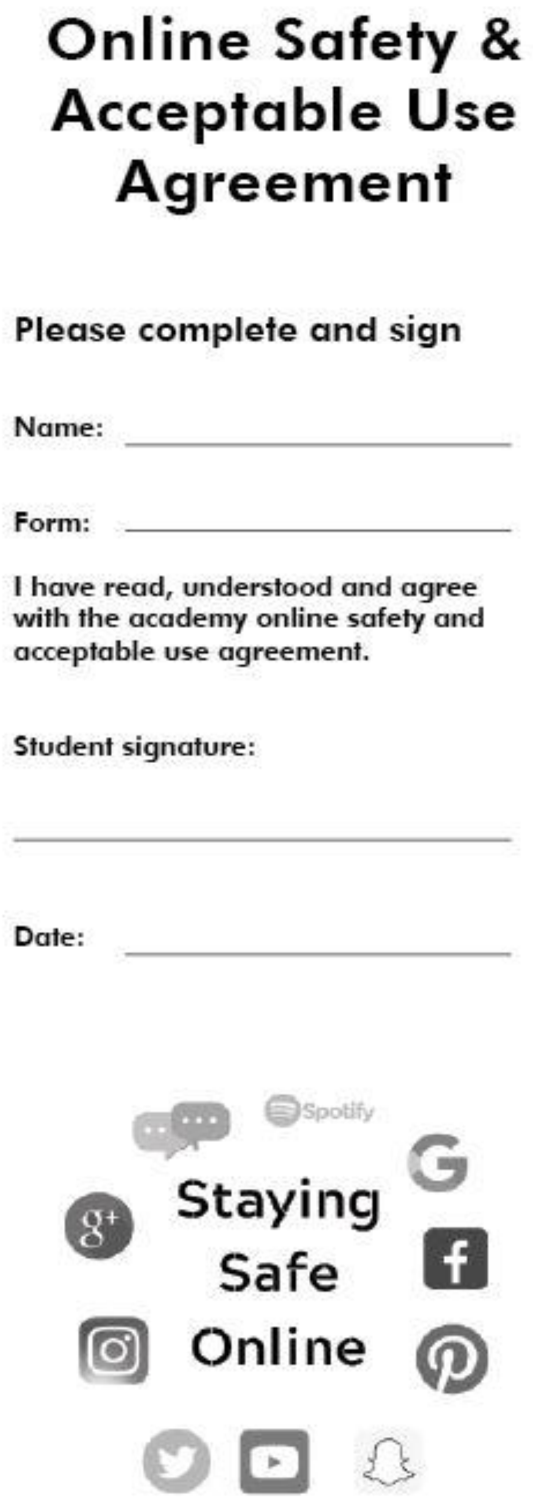
Appendix 1 - Online Safety & Acceptable Use Agreement

Online Safety & Acceptable Use Agreement

This agreement has to be signed by all students. It is also on the academy website and is supported by the academy Child Protection policy.

1. I will not supply my personal email address for any educational software. I will only use my CGA address.
2. I will only use ICT systems in the academy, including the internet, email, digital video, Google classroom and mobile technologies, for academy educational purposes.
3. I will not download or install software on academy technologies without staff permission, including music and videos.
4. I will only log on to the academy network, other systems and resources with my own user name and password. I will not share my password or links (MST) with anyone.
5. I will follow the academy's ICT security system and will not reveal my passwords to anyone.
6. I will make sure that all ICT communications with students, teachers or others are polite, responsible and sensible.
7. I will not use the internet to bully, hurt or upset others.
8. I will not browse, download, upload or forward material that could be considered offensive, inappropriate or illegal. If I come across any such material, I will report it to a member of staff or online platform immediately.
9. I will not give out any personal information online, enter chat rooms or play inappropriate internet games.
10. I will not arrange to meet people I have only been communicating with online.
11. I am aware that if I have been given permission by a member of staff to take images of students and/or staff during academy activities on or off site, I must only store and use these for academy purposes and must never distribute these outside the academy network without the consent of all parties involved.
12. I will ensure that my online activity, both in and outside the academy, does not bring the academy community into disrepute.
13. I will always respect the privacy and ownership of others' work online.
14. I will not attempt to bypass the internet filtering system.
15. I understand that all my use of the internet (including materials sent and received) and other related technologies can be monitored and logged and can be made available to my teachers.
16. If I bring a Smart Watch into the academy, I will ensure that it is used according to the expectations set out in this online safety and acceptable use policy.
17. I will not move or cause damage to any of the hardware (e.g. monitor, hard drive, mouse etc.)
18. I will not sign up to online services until I am old enough to do so.
19. I understand that if these rules are not followed, academy sanctions will be applied and my parent will be contacted.
20. I am aware of how to report concerns online: www.ceop.police.uk/safety-centre
21. For immediate help, I know that I can contact my local police on 101, the Children Exploitation and Online Protection safety centre (CEOP.police.uk) or, if I have a real emergency, I can call 999.

Appendix 1 - Continued Online Safety & Acceptable Use Agreement



Online Safety & Acceptable Use Agreement

Please complete and sign

Name: ______________________________

Form: ______________________________

I have read, understood and agree with the academy online safety and acceptable use agreement.

Student signature:

____

Date: ______________________________

Staying
Safe
Online

Appendix 2 - Your Internet - staying safe online

You have the right to always feel safe - during the academy day and outside of school hours. The internet is a great source of information, fun and entertainment but you must make sure that you use the internet **responsibly**.

1. Always respect others - be careful what you say online and what images you send.
2. Take great care with your 'online reputation' - every time you give information on a website, for everyone to see, a little bit of your privacy will disappear.
3. Think before you send - whatever you send can be made public very quickly and could stay online forever.
4. Treat your password like your toothbrush - keep it to yourself. Only give your mobile number or personal email address or social media account names to trusted friends.
5. Always protect your privacy - when creating online profiles for chatting and/or playing games avoid giving your full name, address, telephone number, email and academy name.
6. Use an online nickname and make your online profile private.
7. Choose online friends carefully - someone you have not met in the real world is still a stranger.
8. Block the sender - learn how to block or report someone who is behaving badly.
9. Do not reply to messages that harass or upset you, instead save the evidence - learn how to keep records of offending messages, pictures or online conversations.
10. Make sure you tell someone if something unacceptable does happen. You could tell:
    - An adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence.
    - Your form tutor, a teacher or your engagement support assistant

Remember: Do not neglect the 'real world' - social networking, chatting and online gaming can be great fun but do not neglect your homework, friends, exercise and all the other fun activities and hobbies in the 'offline world'.

Key staff at the time of policy review are:

Anna Feltham, Headteacher afeltham@clapton.hackney.sch.uk

Trustee responsible for safeguarding (including online-safety), Dipti Mouj

Online Safety Co-ordinator (also the Designated Safeguarding Lead)

Dominic Fyles dfyles@clapton.hackney.sch.uk

Head of Computing and ICT, Sonia Rai srai@clapton.hackney.sch.uk (Maternity cover TBC)

ICT support, Shaeid Sharif / Ahmed Patel ITsupport@clapton.hackney.sch.uk

School Business Leader, Helen Edwards hedwards@clapton.hackney.sch.uk

Appendix 3 - How to Protect Your Children on Their Smartphone

Smartphones have plenty of apps to entertain children, help them with their homework, and more. But just like anything else that's connected to the internet, parents need to make sure their children are safe while using smartphones and other smart devices. Here are some tips on how they can do that.

Basic Best Practices

The NSPCC, Net Aware and O2 are dedicated to keeping children safe online.

Parents should speak to their children about what other kids are doing with their phones. This will help parents:

- Understand what their children see as social norms
- Better explain to their children what is and is not appropriate

Parents should set clear guidelines for their children regarding certain topics, including:

Youth Produced Sexual Imagery and Child Sex Abuse Imagery

- Sending sexually inappropriate pictures or messages is not only unacceptable, those messages are permanent and can easily be shared with others.
- Being in possession of, sending or receiving, a youth produced sexual image or a child sexual abuse image, is a crime under U.K. law

Phone-free times

- Consider making certain times, such as family meals or from 9 PM to 8 AM, phone-free times
- Children can place their phone in a certain area, or parents can restrict phone usage at specific times by managing their data plan
- Parents should remove mobile phones from bedrooms when children go to sleep.

Cyberbullying

- Let children know that they can speak to you if someone harasses them online or through text. Tell them about CEOP and what this organisation does (link below)
- Children should also be aware of the harm they can cause by bullying or abusing others
- Children should be made aware of the negative effects of creating a fake social media account, in order to disparage or harm another person.

Sharing their personal information

- Personal information, such as full name, address, or phone number should:
- Never be given out to strangers
- Not be posted online where anyone can see it

Making in-app purchases

- Many apps (not just games) allow users to purchase additional content and features
- Children should know whether they are allowed to make purchases, and if not, the consequences for purchasing things without parental permission

In addition to speaking to their children, parents can go through their service providers and directly manage smartphone usage through their data plan. Many service providers allow parents to:

- Set limits on texts, data, purchases or voice minutes
- Receive alerts on phone activity
- Monitor number of texts and other usage
- Review and block contacts
- Review apps (and add money to be used to purchase apps)
- Lock phone usage on-demand or at specific times
- Block harmful or inappropriate websites on their home WiFi and mobile phone accounts.

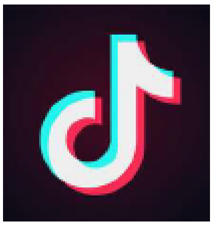
N.B. Please be aware that children may be able to get around parental settings by accessing public Wi-Fi.

How to Keep Kids Safe on Popular Apps

The UK Council for Internet Safety (UKCIS) was set up to help everyone safe online and work with services like CEOP and the NSPCC. Facebook and Snapchat require their users to be at least 13 years old and other apps will have the same age restrictions. Parents must be aware that children can lie about their age to access apps that are not within their age group.

If parents allow their children to use these apps, they should know the following:

Most popular apps



TikTok is a global video community powered by music. Whether it's dance, free-style or performance, users are encouraged to let their imagination run wild and express themselves as they wish.

Houseparty is a group chat app. When the user and their friends are in the app at the same time, they'll see each other instantly. One tap and they're in. Users could be in a group chat with their friends and people that they do not know.

Instagram is a photograph and video sharing app. Instagram is one of the most popular apps in the UK. Users can share videos and photographs of themselves, and livestream videos to their followers. Profiles can be private or publicly shared.

Twitch is a live video game website. Users can watch playbacks of games being played by other people. Users can also live stream their own games.

Discord is the only cross-platform voice and text chat app designed specifically for gamers. It is perfect for chatting with team members and seeing who is playing online. Not all team members would be known to the user.

On **Snapchat**, users can send photos and videos that delete themselves after a few seconds. This may encourage inappropriate content being recorded as users are less concerned because the content will be deleted. However, content can be retrieved.

Whatsapp is an encrypted, personal messaging app. Users can share messages, photographs, videos and voice notes with contacts that they have in their phone address book. Message settings can be changed, so that messages disappear after 24 hours should a user choose this. Users can also broadcast videos and images to all their contacts via status updates.

Youtube is a video sharing platform. Users can watch videos on a wide range of subjects. Users can also share videos with the rest of the Youtube community. There is no age limit to use Youtube.

Most concerning apps

Meta

Facebook Metaverse is a platform in which users can interact with other users via an avatar and their facebook VR headset. Users can play games and interact in various virtual settings. As the metaverse is new, there are very few regulations and laws governing how people behave, or how adults can access children.

Yubo allows users to meet new people around the world. Make new friends, chat and meet new people. Right to like, left to pass; just like Tinder. If two people like each other's pictures, they can chat live.

AskFM is an anonymous messaging app, in which users can put out questions that people respond to anonymously. Children should be encouraged to always avoid anonymous messaging apps, as these apps open easy channels for bullying

Monkey allows users to talk to strangers. Users can facetime strangers from anywhere. Monkey stories can be created and viewed by tapping the tree. Users can send a friend request if they like what they hear or see.

Secret Calculator hides photos, contacts and videos behind a calculator icon. If users put in a passcode it will open a private area. Users can browse the internet without the history being saved.

Appendix 4 - Advice for parents

Advise your child to:

- Use a strong password
- Use a different name and avoid using personal images
- Not include any of their personal information
- Block and report any inappropriate content- show them how to do this
- Use privacy settings- show them how to do this
- Not use apps that are not for their age group- check this with them
- Not accept friend requests from strangers
- Switch off location services
- Think before they post

The NSPCC and Net Aware links below have useful guidelines and advice about the most popular apps.

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

https://www.net-aware.org.uk/networks/?order=title

CEOP is a law enforcement agency and is there to help keep children and young people safe from sexual abuse and grooming online. They help thousands of children and young people every year.

https://www.ceop.police.uk/safety-centre/

UKCIS previously known as UKCCIS, now works to provide everyone with guidance about online safety.

https://www.gov.uk/government/organisations/uk-council-for-internet-safety