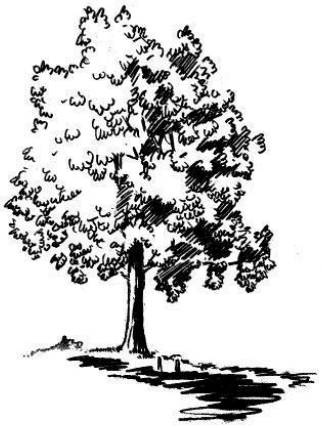
Blossom Lower School and Upper House



Online Safety Policy

EYFS, Primary, Secondary and Post 16

Clementine Turner-Powell

Fiona Roberts

Georgette Maile-Shadbolt

Harriet Palmer

Viviana Patterson

Last reviewed September 2021 (by above staff)

Next review due September 2022

Whole-school approach to online safety

At Blossom House School, we recognise that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face, and in many cases, abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Blossom House School facilitates a whole-school approach to keeping children safe online. Whilst online safety is a running and interrelated theme in all of our school's policies and procedures, this policy aims to make clear how the school supports pupils, parents and staff to make online safety a priority, the school's expectations in relation to pupils' appropriate use of digital devices and social networking sites, and how any online safety concerns are responded to and managed accordingly.

The school recognises that technology, and risks and harms related to it, evolve and change rapidly. This policy is updated at least annually, or sooner if required. We review our approach to online safety annually, using the 360 degree safe online safety self-review tool for schools. Online safety risks are also considered in our safeguarding risk assessment.

Digital devices and social networking

Digital devices are physical units of equipment that contact a computer or a microcontroller, such as: mobiles phones, smart watches, iPads and tablets, music devices such as iPods, Kindles, laptops, games consoles, recording devices, devices containing a SIM card, devices that use GPS, or any other smart technology.

Social networking is a way of communicating or messaging using smart technology or digital devices. It may be between individuals and/or groups. Communication can take place on social media platforms such as TikTok, Snapchat, Instagram, Facebook, Twitter or YouTube; text or video messaging apps such as Facebook Messenger, WhatsApp, iMessage or Facetime; gaming consoles with a chat function such as Xbox Live or Nintendo Switch; or any other internet sites which have a comments section, live chat room, or in-game chat facility.

Making online safety a priority

The 4 Cs

Pupils, parents and staff are taught how to recognise online safety risks, and how to get help and escalate concerns where necessary. Our online safety approaches aim to cover the four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **contact:** being subjected to harmful online interaction with other users; e.g. peer to peer pressure, commercial advertising, or 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; e.g. sending and receiving explicit images, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, persistent unwanted contact, or online bullying
- **commerce:** risks such as gambling, inappropriate advertising, phishing, or financial scams (any risks should be reported to the Anti-Phishing Working Group)

Childnet and UK Safer Internet Centre

The school works with Childnet online safety charity to run annual e-safety workshops for pupils, parents and staff. Childnet works with the government and internet industry as experts in the field of online safety education. These workshops look at the potential risks faced by children and young people as they explore the internet, and offer advice around how to take a whole school approach in responding. They also highlight resources to use in the classroom which help to explore and reinforce online safety.

The school also supports the UK Safer Internet Centre's annual Internet Safety Day, celebrated globally in February each year to promote the safe and positive use of digital technology for children and young people and inspire a national conversation. It calls upon young people, parents, carers, teachers, social workers, law enforcement, companies, policymakers, and wider, to join together in helping to create a better internet.

IT filtering and monitoring

In order to provide a safe learning environment, our IT filtering systems and do all they reasonably can to limit exposure to the main areas of risk and safeguard against cyber-crime technologies. Monitoring and screening systems will raise an alert should anyone attempt to access or share inappropriate material. Specific sites can be blocked during school hours should these present any safety concerns, or become a cause of distraction from learning.

Online safety for pupils

All children are vulnerable to accessing and engaging with potentially harmful and inappropriate online material, and we recognise the additional risk posed to children with SEN. Due to the nature of our pupils' speech, language and social communication difficulties, many of our pupils do not recognise the potential safety risks they may face online. Online safety is therefore an area that continues to be revisited and reinforced throughout the school curriculum, through pastoral support sessions, or in 1:1 therapies.

Pupils are taught about online safety through various teaching, learning and therapy opportunities, which includes helping them to be clear about what is expected of them online as well as offline. Internet safety and cyber bullying issues as taught as part of the ICT and PSHE curricular. This includes safety regarding the use of webcams in computers (and programmes such as Skype) as well as the distribution of photos/images on various sites. Pupils are taught skills such as how to block or report another person who sends them friend requests or messages which they do not like or are offensive.

Through the use of circle time, pupils are offered the opportunity to discuss issues that may arise whilst being online. This forum allows pupils to support each other in thinking about the risks and identifying who to turn to if concerned.

Where pupils are required to access learning or therapies remotely, protocols in the *Remote Working and Dual Provision Policy* will be followed.

Online safety for parents

As a school, we rely on parents to monitor and maintain close supervision of their child's digital devices, social networking, and internet use outside of school hours. This may include setting up parental controls and filters, removing or restricting access to devices, and/or blocking specific sites or apps if necessary.

Parents of children in KS2 upwards are sent an ICT and Social Networks contract to sign, thereby agreeing to the school rules around online safety.

In addition to the annual e-safety workshops run by Childnet, the school offers regular e-safety updates for parents, to help them to keep their children safe online. This policy will be made available to parents via the school's website.

Online safety for staff

Policies are in place to support staff to make online safety a priority. Please refer to our *Mobile Phone Policy for Staff*, *Staff Code of Conduct*, and *Remote Working and Dual Provision Policy*.

Expectations for pupils

Whilst we make every reasonable effort to safeguard children from accessing and engaging with potentially harmful and inappropriate online material at school, we recognise that most pupils bring digital devices to school, therefore have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). The use of digital devices (with or without internet access) can cause a distraction to learning, and/or pose a safeguarding risk to our pupils and/or their peers. We aim to address this by setting expectations for pupils, and having clear procedures to follow where these expectations have been breached.

All pupils up to and including year 10 are not allowed to use digital devices in school (except where these have been deemed necessary to support pupil wellbeing e.g. music devices, apps for calming etc.). Digital devices, including mobile phones and smart watches, must be handed into Group Leaders during morning registration and are returned at home time. Mobile Phones may sometimes be required in a lesson such as Functional Skills, however would only be used only at the request and under the guidance of the teacher or therapist. If a pupil does not hand a phone in, then their Specialist Advisor is made aware who can contact home to discuss this further. Every new pupil from KS2 upwards signs an ICT and Social Networks contract, thereby agreeing to the school rules around online safety.

In Year 11 pupils are allowed to keep their digital devices in their lockers, and they may wear smart watches as long as they are switched onto airplane mode. They may also use their mobile phones and keep them in their pockets. They can use their phones for organisation reasons, to photograph work to support their learning as well as to download specific coursework related photographs under the strict supervision of the teacher. These allowances may be removed if pupils do not adhere to the rules.

In Post 16, communication needs are different, as staff/students need to be in contact whilst on their college placement. There is also a greater focus on developing independence, e.g. independent travel. Post 16 students may keep their phones about their person, but they may only be used at break times or when off-site. They must never be used during lesson times, unless at the request and under the guidance of the teacher or therapist. If a student does not respond to warnings to put their phone away, their phone must be handed in until the end of the day. There are signs up in each classroom reminding students of this rule.

Expectations for pupils are reinforced through ICT, Functional Skills, Life Skills and PSHE sessions, as well as ad hoc discussions during Group Times or 1:1 with the Group Leader. On occasion, 1:1 SLT or RSE support may be needed to aid pupil understanding. All staff are encouraged to remind pupils of the expectations for their key stage.

Online Safety Rules

The school recognises that due to the nature of our pupils' speech, language and social communication difficulties, any rules regarding their use of digital devices and social networking need to be explicit, clear and consistent, as far as is possible.

- Pupils are not allowed to contact staff on any social media platforms
- Pupils are not allowed to use their friend's social media accounts to contact staff
- Pupils are not allowed to make false accounts to contact staff
- Pupils are not allowed to write or upload any material about a member of staff on their social media platforms
- Pupils are not allowed to write or upload any material which is rude or disrespectful about the school, staff, or pupils on their social media platforms
- Pupils are not allowed to use any social media platforms to encourage unkind or inappropriate comments about another pupil, to write derogatory or unkind comments about another pupil, or to use it to arrange or encourage bullying behaviours
- Pupils are not allowed to use any social media platforms to share any unsuitable material with, or about their peers
- Pupils are not allowed to join in with any bullying related communication
- Pupils are not allowed to use digital devices or social networking to harass other pupils or staff either inside or outside of school. *Harassing* includes contacting lots of times, contacting after being asked to stop and/or contacting with the intention of causing the other distress or upset
- Pupils are not allowed to use digital devices in any of the toilets on school premises
- Pupils are not allowed to use digital devices to record whilst on school premises
- Pupils are not allowed to record or take photos of staff or other pupils without their knowledge or consent

Responding to online safety concerns

Where expectations for pupils or online safety rules have been breached, the school follows clear procedures *(please see flow chart for consequences for different behaviours involving social networking and digital devices in* ***Appendix 1****).* The school will consider the pupil's intentions and possible social misunderstandings, in line with their speech, language and social communication difficulties. Where necessary, the school will adhere to statutory guidance published by the DfE.

The pupil(s) involved may be required to meet with the Principal, Joey Burgess. Parents will be contacted and may also be asked to attend such a meeting. Appropriate support and/or consequences will be agreed, depending upon the nature of the incident.

We aim to support communication breakdowns, and help repair issues that have arisen, through group PSHE and/or 1:1 speech and language therapy sessions. The Restorative Justice team may be called upon, if appropriate, as a supportive way for pupils, parents, or staff members to feel heard, develop reflective skills to learn from the incident and move forwards positively. As with all behaviour, a restorative approach is used alongside consequences to support reflection and learning and moving forwards to supporting pupils to make safer and more positive choices. Where there is conflict between pupils, Restorative Justice can empower them with the skills to fix the damage caused and repair relationships.

Where the use of social networking has been used as a means of cyber bullying, procedures in our *Anti-Bullying Policy* will be followed. Please also see *Peer on Peer Abuse*.

Where pupils are at risk of being harmed or of causing harm to others who are not part of Blossom House School, safeguarding protocols will be followed.

Responding to safeguarding concerns Please refer to our *Safeguarding Children and Child Protection Policy*.

Child Sexual Exploitation (CSE)

CSE is a form of child sexual abuse. It may include non-contact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet. CSE can occur over time or be a one-off occurrence, and may happen without the child's immediate knowledge e.g. through others sharing videos or images of them on social media**. If CSE is suspected, the DSL should be informed immediately.**

Peer on Peer Abuse

Where children abuse other children, this is referred to as peer on peer abuse. Online peer on peer abuse is most likely to include, but is not limited to:

- cyberbullying bullying, which includes prejudice-based and discriminatory bullying
- facilitating, threatening and/or encouraging physical harm
- facilitating, threatening and/or encouraging sexual violence

• online sexual harassment, such as sexual comments, remarks or jokes, which may be stand-alone or part of a broader pattern of abuse
• causing someone to engage in sexual activity without consent, including forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
• consensual and non-consensual sharing of nudes and semi nudes images/videos (also known as sexting or youth produced sexual imagery);
• upskirting, which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; and
• initiation/hazing type violence and rituals, including online activities involving harassment, abuse or humiliation

Where peer on peer abuse is suspected, or where an allegation has been made, the DSL should be informed immediately. If a potential criminal offence has taken place, the Police will also be contacted.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
• denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the DSL should be informed immediately. A referral to the Cyber Choices programme may also be considered.

For more information on keeping children safe online please see *Annex D of Keeping Children Safe in Education.*

Latest D.f.E Guidance:

- Keeping Children Safe in Education (2021)
- Sexual violence and sexual harassment between children in schools and colleges (2021)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (2020)
- Searching, screening and confiscation: advice for schools (2018)
- Preventing and tackling bullying: Advice for headteachers, staff and governing bodies (July 2017)
- Teaching Online Safety in School 2019

Other policies of relevance:

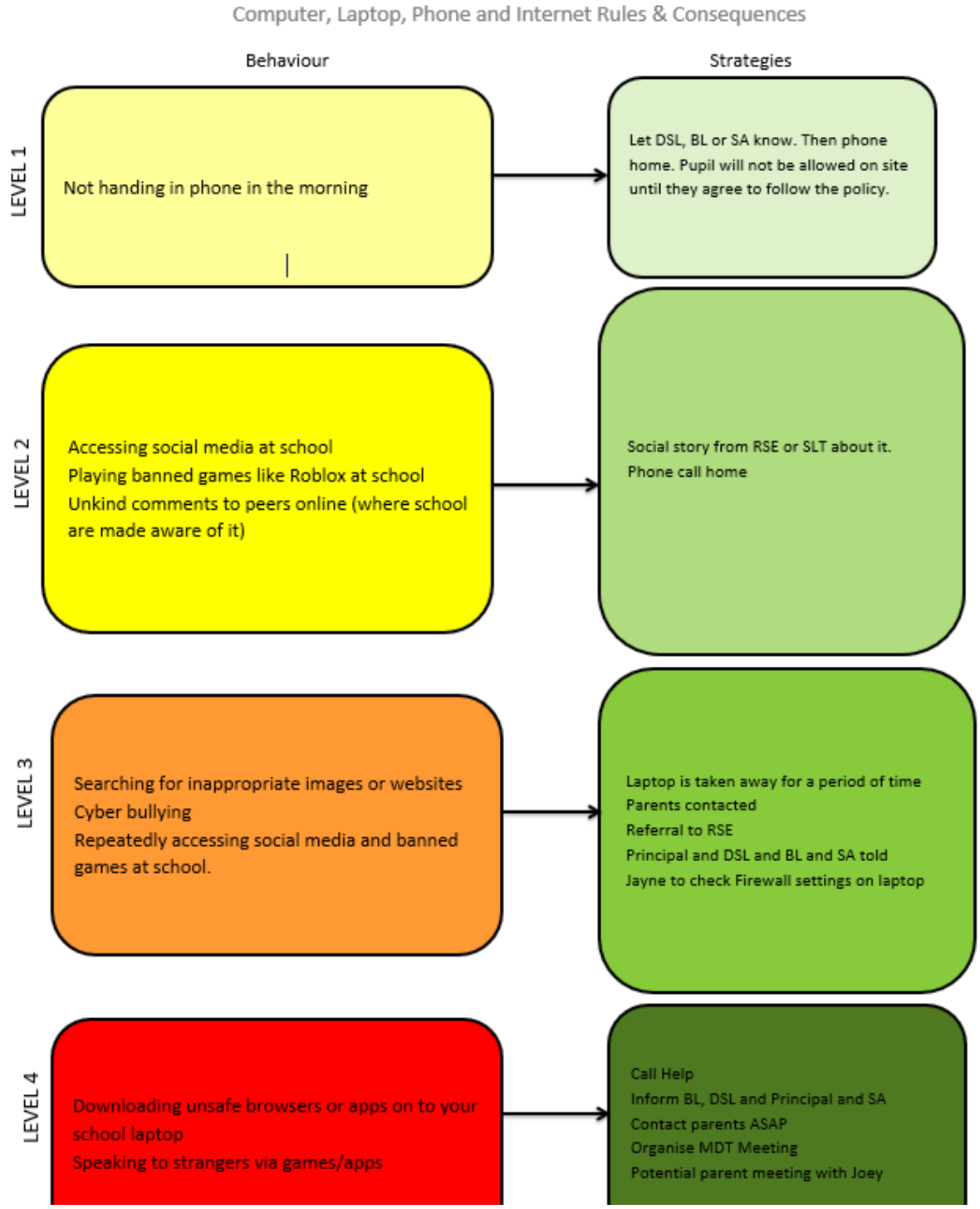
Behaviour Management

Anti-Bullying

Safeguarding and Child Protection

Remote Working and Dual Provision Policy

Appendix 1: Flow Chart for Behaviour and Consequences



Appendix 2: Social Network and Phone Contracts sent to Pupils

Blossom House School ICT and Social Networks Contract (pupils & parents to sign)

1. I will only use the school's computers for schoolwork and homework. **I am awa that the use of any school computer, telephone or communications facility fo any unauthorised activity is against School policy and may even be a criminal offence.**

2. **I will not use ICT / social network sites within or outside school to bully others (this could include sending unkind or threatening messages, or posting information to upset pupils and/or staff, this includes creating groups) and I am aware of the laws linked to cyber bullying.**

3. **I will not access, create, download, copy, print or share any material that may be considered to be racist, sexist, obscene, violent or bullying, or make nasty or hurtful comments about other pupils and/or staff on any social network site.**

4. I understand that social networking and gaming sites cannot be used in school unless permission has been given by an adult.

5. **I will not log on with anyone else's user ID and password and I** will only edit or delete files in my user area.

6. I am aware of the dangers of giving out personal details such as: name, address, photos, telephone number, bank account, on the Internet or by e- mail.

7. **I will behave sensibly in computer rooms and treat the equipment with respect.**

8. **I will not attempt to contact or add staff on any social network sites. I am aware doing this is against school policy.**

I have read and understand these rules and agree to them.

Name:……

Group:……

Signed parent:……

Signed pupil:……

Date:……

Blossom House School mobile phone contract (pupils and parents to sign)

1. I will turn my phone off and put it away before entering the school playground in the morning.

2. If I am in Years 7-9, I will hand my phone to an adult as soon as I enter the classroom for morning registration.

3. If I am in Years 10-11, I will put my phone away in my locker or bag and leave it there for the day.

4. I will not use my phone to take or distribute photos / videos of school property.

5. I will not use my phone to take or distribute photos / videos of other pupils and/or staff.

6. I will not use my phone to access the internet or social networking sites during the school day.

7. I will not use my phone to contact / talk to friends during the school day.

8. I understand that if I am not following the mobile phone rules, school will contact my parents and I will be given an appropriate consequence.

I have read and understand these rules and agree to them.

Name:.....

Group:.....

Signed parent:.....

Signed pupil:.....

Date:.....