



## St Andrew's CEVA Primary School Online Safety For Pupils Policy

### Background & Rationale

St. Andrew's Church of England Primary School is committed to providing a thriving Christian environment through the I ASPIRE values. These reflect the Christian ethos of our school and ensure that everyone feels safe, valued and supported so that all individuals can reach their highest goals and are encouraged to engage in lifelong learning. Our vision statement "*With God all things are possible*" (Matthew 19:26) is at the core of our values and is used to inspire everyone to be open to all possibilities and have a positive attitude and outlook to life. Spiritual, moral and emotional development are central to the life of our school and this will be reinforced in the School's Online Safety for Pupils Policy where appropriate.

### Introduction, Key People and Dates.

St. Andrew's CEVA Primary School	Designated Safeguarding Lead (DSL) team	Sue Gentry, Michelle Davidson, Val Griffiths, Florette Francis, Michelle Day and Rosie Spikings.
	Online-safety lead (if different)	Sue Gentry & Aimee Jones
	Online-safety / safeguarding link governor	Pete Lightfoot
	PSHE/RSHE lead	Selena Hodson
	Network manager / other technical support	Graham Underlin
	Date this policy was reviewed and by whom	September 2022 Aimee Jones & Sue Gentry
	Date of next review and by whom	September 2023 Aimee Jones & Sue Gentry

### Aims

This policy aims to:

- Set out expectations for all St. Andrew's CEVA Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all members to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Safeguarding and Child Protection Policy)

## **Scope**

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with '[Keeping Children Safe in Education' 2022 \(KCSIE\)](#)', '[Teaching Online Safety in Schools' 2019](#)' and statutory [RSHE guidance 2021](#) in addition to other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; and is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety will follow the school's safeguarding and child protection procedures.

At St. Andrew's this policy will be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. We advise that all staff members have read the [DFE guidance](#) at the beginning of each academic year alongside the updated Online Safety policy, Safeguarding and Child Protection policy and Acceptable Use policy to see what needs changing in the light of potential closure, remote learning and alternative arrangements at school. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy as suggested in KCSIE (2022). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils will set their rules on how to keep safe online at part of an Online Safety introduction at the beginning of each academic year, with the expectation to discuss this with their parents / carers at home (see appendices).

Acceptable Use Policies (see appendices) for different stakeholders help us to keep all members on site safe and we will ensure that these are reviewed alongside this overarching policy. Any changes to this policy will be immediately disseminated to all the above stakeholders.

## **Roles and Responsibilities**

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

### **Head teacher – Mrs Val Griffiths**

#### **Key Responsibilities:**

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguarding concerns.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

### **Designated Safeguarding Lead – Sue Gentry & Online Safety Lead – Aimee Jones**

#### **Key Responsibilities:**

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead** responsibility should not be delegated”
- Work with the Headteacher and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.
- Regularly review and have an open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure that the Online Safety Policy is communicated to the school community, in addition to their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate.
- Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation and be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance, and beyond, in wider school life

- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents
- Communicate regularly with SLT and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure Guidance such as the [sharing of nudes and semi-nudes](#), is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Oversee and discuss the filtering and monitoring of internet searches through the use of SafeSearch.
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE 2022 Part One and Annex B

### **Governing Body, led by Online Safety and the Safeguarding team.**

#### **Key Responsibilities**

- Approve this policy and strategy and subsequently review its effectiveness.
- Ask about how the school has reviewed protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.
- “Ensure an appropriate **senior member** of staff, from the school is appointed to the role of DSL with **lead responsibility** for safeguarding and child protection (including online safety) with the appropriate status and authority [and] time, funding, training, resources and support...”
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part One of KCSIE 2022 & Annex B; SLT and all working directly with children have read Annex B; including Online Safety and checking it reflects the practice in our school
- “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice from the local three safeguarding partners and integrated, aligned and considered as part of the overarching safeguarding approach.”
- “Ensure appropriate filters and appropriate monitoring systems are in place [but...] be careful that ‘overblocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology.”

### **All Staff**

#### **Key Responsibilities**

- In 2022 pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies**.
- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Part 1 and Annex B of Keeping Children Safe in Education 2022 staff.
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL if the policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying, sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

#### **RSHE lead – Selena Hodson**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the RSHE curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where

- to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within RSHE.
- Note that an RSHE policy should now be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

## **Computing Lead – Aimee Jones**

### **Key Responsibilities**

- As listed in the ‘all staff’ section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

## **Network Manager & Technician – Graham Underlin**

### **Key Responsibilities**

- As listed in the ‘all staff’ section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home and remote-learning** procedures, rules and safeguards.
- Keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school’s online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school’s systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

## **Data Protection Officer – Plumsun**

### **Key Responsibilities:**

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents '[Keeping Children Safe in Education](#)' and '[Data protection: a toolkit for schools](#)' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

## **Volunteers and contractors**

### **Key Responsibilities:**

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

## **Pupils**

### **Key Responsibilities:**

- Read, understand, sign and adhere to the student acceptable use policy and review this annually
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

## **Parents / Carers**

### **Key Responsibilities:**

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns

## **External groups including parent associations**

### **Key Responsibilities:**

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

## **Online Safety in the curriculum**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

At St. Andrew's CEVA Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety) through the use of Project Evolve and Google: Be Internet Legends.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

## **Handling online-safety concerns and incidents.**

### **The 4C's**

Our Online Safety Policy explores the **Content, Contact, Conduct or Commercialism** identified in '[Keeping Children Safe in Education](#)', 2022. These four areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three. It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and RSHE).

Many of these new risks are mentioned in [KCSIE 2022](#), e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

This policy takes into account the government's investigation into **peer-on-peer sexual abuse** and [Ofsted review](#), our school has reviewed our policies to ensure appropriate processes are in place to allow pupils to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately. We have ensured that all parents and careers are aware of the following websites to report online safety concerns: [Childnet](#), [Internet matters](#), [NSPCC: Online Safety](#), [Think U Now](#) and [LGfL DigiSafe](#).

We ensure parents receive regular online safety updates through our social media sites: Twitter, Facebook and School Website. Here they can find guides on how to discuss concerns with their child and how to update privacy settings on their child's social networking accounts.

### **Staff Expectations**

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Peer on Peer Abuse Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- RSHE policy
- Staff code of conduct

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school.). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

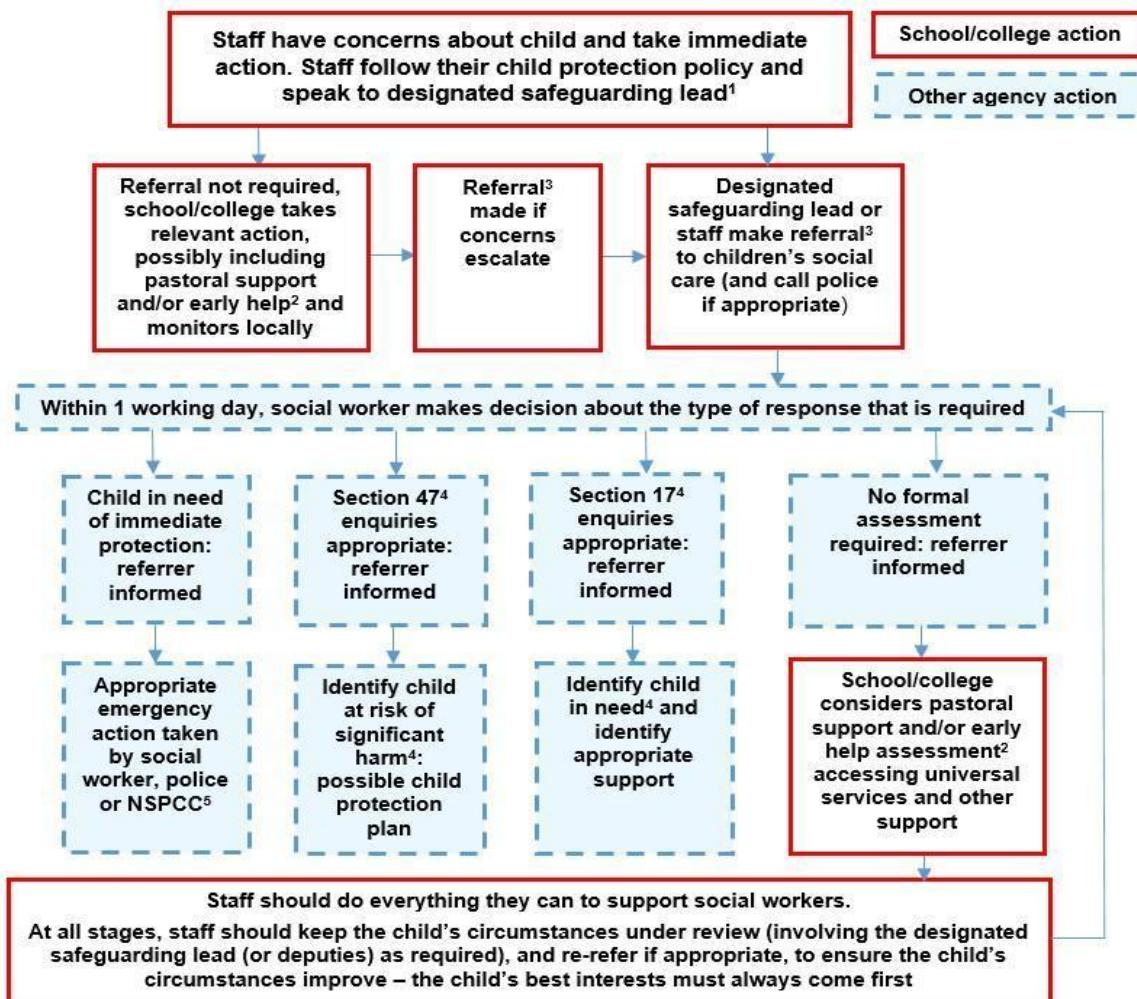
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the [NSPCC Whistleblowing Helpline](#).

The school will actively seek support from other agencies as needed. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

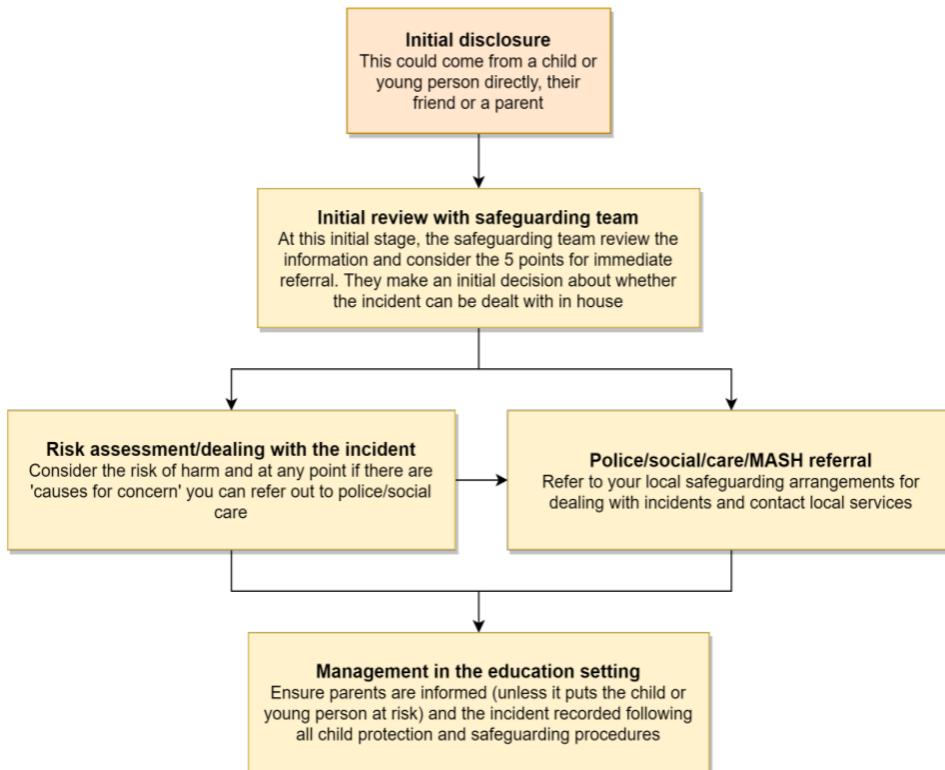
### **Actions where there are concerns about a child**

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



### **Sexting – Sharing nudes and semi-nudes**

Our staff all follow the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#) in order to avoid unnecessary criminalisation of children. This enables them to follow the correct procedures and ensure that the school's DSL has the information needed to decide the next steps and whether other agencies need to be involved.



#### \*Consider the 5 points for immediate referral at initial review:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involve sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

Staff and school community members are aware that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area

#### **Upskirting**

In our school we make it a priority that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in [Keeping Children Safe in Education](#) and that pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

#### **Bullying**

"Cyberbullying is any form of bullying which takes place online or through smartphones and tablets. Social networking sites, messaging apps, gaming sites and chat rooms such as Facebook, XBOX Live, Instagram, YouTube, Snapchat and other chat rooms." (BullyingUK, 2020). [The Education and Inspections Act \(2006\)](#) states that Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils that are off site. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour.

There are many types of cyber-bullying (BullyingUK, 2020):

- **Harassment** – Sending offensive, rude and insulting messages and being abusive. This can be carried out by commenting on posts, photos and / or in chat rooms.

- **Denigration** – Sending information about another person which is fake, damaging and untrue. In addition to sending photos of someone to spread fake rumours, gossip or ridicule.
- **Flaming** – Someone who is purposefully using extreme and offensive language to get into online arguments and / or fights.
- **Impersonation** – When someone hacks into someone's email or social networking account and using their identity to send or post material to / about others.
- **Outing and Trickery** – Someone shares personal information about another to trick someone into revealing secrets. This may also be done using private images / videos.
- **Cyber Stalking** - Repeatedly sending messages that includes threats of harm, harassment, intimidating messages or engaging in online activities which make a person afraid for their safety.
- **Exclusion** - Intentionally leaving someone out of a group such as group messages, online apps, gaming sites and other online engagement.

### **Preventing Cyberbullying and supporting an individual who is being bullied**

It is important that as a school we work in partnership with the pupils and parents to educate them about Cyberbullying, all individuals should understand how to use a range of technologies safely and show an awareness of the risks and consequences of misusing them. Know what to do if they or someone is being cyber bullied and report any problems which arise.

Additional online advice on Cyberbullying can be found on: <https://www.nationalbullyinghelpline.co.uk/> or <https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/>

When supporting individuals who are being bullied support will be given in line with our school's behaviour policy. All incidents will be investigated fully and parents will be informed of the actions that we have taken place in school.

### **Sexual Violence and Harassment**

All staff members are aware of the DFE in Keeping Children Safe in Education and have received guidance on paragraphs 45-49 which cover the immediate response to a report and confidentiality should an issue arise.

Any incident of sexual harassment or violence (online or offline) will be reported to the DSL who will follow the full guidance. Staff to foster a zero-tolerance culture. As a school we take all forms of sexual violence and harassment seriously, and are aware that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

### **Misuse of school technology (devices, systems, networks or platforms).**

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to bring your own device.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

As a school we will highlight these at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, as a school we reserve the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

### **Social media incidents**

Please see the Child Protection and Safeguarding policy on how online incidents are dealt with. Please also refer to the staff and pupil acceptable use policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). Incidents will be recorded on Edukey our safeguarding system.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the [Professionals' Online Safety Helpline](#), POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

### **Remote Learning**

In any potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some of our pupils may miss opportunities to disclose such abuse during the lockdowns or periods of absence. In any remote learning period we will make it our priority to continue to teach our students the importance of staying safe online, by enhancing their understanding of critical thinking and digital resilience.

### **Policy Communication**

It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

### **Data and protection and data security.**

GDPR information is monitored by the school bursar and our data controller is Plumsun.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

**"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information**

**with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.”**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here.

The headteacher, data protection officer and governor's work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

As a school we conform to GDPR regulations in relation to:

- CCTV
- Use of personal vs school devices
- Password protection – forced regular changes
- Reminders to lock devices when leaving unattended
- Device encryption
- Access to and access audit logs for school systems
- Backups
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies
- Wireless access
- File sharing
- Google Drive use, access and sharing protocols

### **Appropriate filtering and monitoring**

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, the internet connection is provided by BT. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called SafeSearch, which is made specifically to protect children in schools.

When pupils log into any school system on a personal device, activity will also be monitored here.

### **Social Media**

At St. Andrew's CEVA Primary School we work on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first ‘googling’ the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Michelle Day is responsible for managing our website and Facebook page and Computing Lead Aimee Jones is responsible for managing our Twitter account.

### **Staff, pupils' and parents' Social Media presence**

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but our school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, our school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Pupils are not allowed\* to be 'friends' with or make a friend request\*\* to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

\* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

\*\* Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

### **Device Usage**

Reminders are given to those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

#### **Personal devices including wearable technology and bring your own device**

- **Pupils/students** in KS2 students are allowed to bring mobile phones in for emergency use only. During the school day, phones must remain turned off at all time. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to immediate confiscation of the device and immediate contact with Parents, this could also lead to the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they must notify the headteacher beforehand.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, parents will be given information following the permission of the headteacher. They are also asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

### **Trips / events away from school**

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the head teacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

### **Searching and confiscation**

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Head teacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.

### **Appendices**

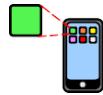
Acceptable use policies



## What I Must do to Keep Safe Online and With Devices



Online means anything connected to the internet. Most devices and apps are



connected to the internet.



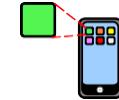
Devices are technology like: computers, laptops, games consoles,



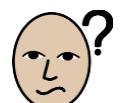
tablets and smart phones.



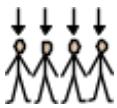
I will only use the devices I am allowed to use.



I will ask a trusted adult before I use new websites, games or apps.



I will ask for help if I'm stuck or not sure.



I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



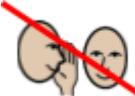
I will tell a trusted adult if I feel bad or unsafe when I am using a device.



I know people online sometimes tell lies.



They might lie about who they are or where they live.



I never have to keep secrets from my trusted adults.



I will not change clothes or undress in front of a webcam.



I will always ask a trusted adult before telling anyone my private



information or location.



I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.  
This could make me feel sad or embarrassed.



   
My trusted adults are \_\_\_\_\_ at school 

   
My trusted adults are \_\_\_\_\_ at home 



My name is \_\_\_\_\_

## **KS1 ACCEPTABLE USE POLICY**

My name is \_\_\_\_\_

To stay **SAFE online and on my devices**, I follow the 4D's and:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

My trusted adults are:

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Name of Pupil: \_\_\_\_\_

Class: \_\_\_\_\_

Apps / Games they use \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

## **KS2 ACCEPTABLE USE POLICY**

1. **I learn online** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. **I learn even when I can't go to school because of coronavirus** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. **I ask permission** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. **I am creative online** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. **I am a friend online** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. **I am a secure online learner** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. **I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. **I know it's not my fault if I see or someone sends me something bad** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. **I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about.
11. **I know new online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. **I check with a parent/carer before I meet an online friend** the first time; I never go alone.
13. **I don't do live videos (livestreams) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. **I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. **I say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~

**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at school that includes**

---

**Outside school, my trusted adults are \_\_\_\_\_**

I know I can also get in touch with [Childline](#)

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Name of Pupil: \_\_\_\_\_

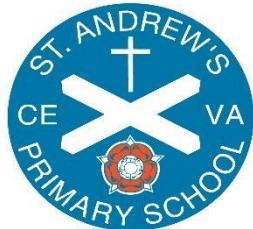
Class: \_\_\_\_\_

Apps / Games they use \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

**STAFF ACCEPTABLE USE POLICY**



**St Andrew's CEVA Primary School  
Staff Acceptable Use Policy**

**Background & Rationale**

St. Andrew's Church of England Primary School is committed to providing a thriving Christian environment through the I ASPIRE values. These reflect the Christian ethos of our school and ensure that everyone feels safe, valued and supported so that all individuals can reach their highest goals and are encouraged to engage in lifelong learning. Our vision statement "*With God all things are possible*" (Matthew 19:26) is at the core of our values and is used to inspire everyone to be open to all possibilities and have a positive attitude and outlook to life. Spiritual, moral and emotional development are central to the life of our school and this will be reinforced in the School's Acceptable Use Policy for staff, governors and volunteers where appropriate.

We ask all children, young people and adults involved in the life of St. Andrew's CEVA Primary School to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and you will be asked to sign it upon entry to the school and every time changes are made.

**Why do we need an AUP?**

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy is detailed in the full Online Safety Policy.

### **Where can I find out more?**

All staff, governors and volunteers should read St. Andrew's CEVA Primary Schools full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies.

If you have any questions about this AUP or our approach to online safety, please speak to our Headteacher Mrs Val Griffiths

### **What am I agreeing to?**

1. I have read and understood St. Andrew's CEVA Primary Schools full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead or Headteacher.
3. During remote learning:
  - I will not behave differently towards students compared to when I am in school. I will never attempt to arrange any meeting, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private / direct communication with a pupil.
  - I will not attempt to use a personal system or login for remote learning or set up any system on behalf of the school without SLT approval.
  - I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom. The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background I will do so.
4. I understand that in the past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
5. I understand the responsibilities listed as my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.
6. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored / captured / viewed by the relevant authorised staff members.
7. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media e.g. by:

- Not sharing other's images or details without permission
  - Refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
- I will not contact or attempt to contact any pupil or access their contact details in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same as the headteacher.
  - Detail's on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.
  - I understand the importance of holding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.
  - I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords / logins and other access, never share credentials and immediately change passwords if I suspect breach. I will only use complex passwords and not use the same passwords for other systems.
  - I will not store school-related data on personal devices. USB keys will be encrypted and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
  - I will never use school devices and networks / internet / platforms / other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
  - I will not outwardly support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
  - I understand and support the commitments made by pupils, staff, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
  - I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sanctions on handling incidents and concerns about a child in a general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
  - I understand that breach of this AUP and / or the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

**To be completed by the user**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**To be completed by Mr G. Underwood & Mrs. S Gentry to issue access/usage permissions**

I approve this user to be allocated credentials for school systems as relevant to their role.

**Systems:** \_\_\_\_\_

**Additional permissions (e.g. admin)** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**VISITORS & CONTRACTORS ACCEPTABLE USE POLICY**



**St Andrew's CEVA Primary School  
Parents Acceptable Use Policy**

**Background & Rationale**

St. Andrew's Church of England Primary School is committed to providing a thriving Christian environment through the I ASPIRE values. These reflect the Christian ethos of our school and ensure that everyone feels safe, valued and supported so that all individuals can reach their highest goals and are encouraged to engage in lifelong learning. Our vision statement "*With God all things are possible*" (Matthew 19:26) is at the core of our values and is used to inspire everyone to be open to all possibilities and have a positive attitude and outlook to life. Spiritual, moral and emotional development are central to the life of our school and this will be reinforced in the School's Acceptable Use Policy for volunteers and contractors where appropriate.

We ask all children, young people and adults involved in the life of St. Andrew's CEVA Primary School to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have any questions, please ask.

Further details of our approach to online safety can be found in the overall school Online Safety Policy.

If you have any questions during your visit, we advise that you ask the person accompany you or DSL's Mrs. V. Griffiths, Miss. M Davidson and Mrs. S Gentry.

If questions arise after my visit, I will ask DSL's Mrs. V. Griffiths, Miss. M Davidson and Mrs. S Gentry.

**What am I agreeing to?**

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. I will never attempt to arrange any meeting, without the full prior knowledge and approval or the school, and will never do so discreetly with a pupil. The same applies to any private / direct communication with a pupil.
3. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture devices) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils. If required (e.g. to take photos of equipment or buildings), I will have prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member of staff.
4. If I am given access to school-owned devices, networks, cloud platforms or other technology:
  - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
  - I will attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
  - I will not attempt to contact any pupils / students or to gain any contact details under any circumstances
  - I will protect my username / password and notify the school of any concerns
  - I will abide by the terms of the school Data Protection Policy and GDPR protections
5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
6. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
7. I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils / students and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by the school. If this is the case, the school will ask me to complete Annex A from the UK Council for Child Internet Safety (UKCIS).
8. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead Mrs. S Gentry or Headteacher Mrs. V Griffiths
9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the visitor / contractor:

**I have read, understood and agreed to this policy.**

**Signature/s:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Organisation:** \_\_\_\_\_

**Visiting / accompanied by:** \_\_\_\_\_

**Date / time:** \_\_\_\_\_

To be completed by the school (only when exceptions apply):

**Exceptions to the above policy:** \_\_\_\_\_

**Name / role / date / time:** \_\_\_\_\_

### **Annex A**

This form is provided as a template to stimulate discussions between external visitors and educational settings. Educational settings may wish to amend and adapt according to their needs and should not replace a formal contract.

| <b>PART ONE</b>                                                                                                                                                       | <b>To be completed by the Educational Setting</b>                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Name of educational setting                                                                                                                                           |                                                                       |
| Main contact and role                                                                                                                                                 |                                                                       |
| Date of session                                                                                                                                                       |                                                                       |
| Start time                                                                                                                                                            |                                                                       |
| Duration                                                                                                                                                              |                                                                       |
| Audience                                                                                                                                                              |                                                                       |
| Age / Year / Key Stage<br>(if appropriate)                                                                                                                            |                                                                       |
| Aims of the session                                                                                                                                                   | <ul style="list-style-type: none"><li>●</li><li>●</li><li>●</li></ul> |
| Specific topics to be covered                                                                                                                                         |                                                                       |
| Other relevant information<br>(Including prior knowledge, training, known safeguarding concerns, safeguarding arrangements, member of staff who will be present etc.) |                                                                       |
| <b>PART TWO</b>                                                                                                                                                       | <b>To be completed by External Visitor</b>                            |
| Name of external visitor                                                                                                                                              |                                                                       |
| Contact information                                                                                                                                                   |                                                                       |
| DBS check or equivalent<br>(if required)                                                                                                                              |                                                                       |
| Title of session                                                                                                                                                      |                                                                       |
| Type of session<br>(Assembly, workshop etc.)                                                                                                                          |                                                                       |
| Learning Outcomes                                                                                                                                                     | <ul style="list-style-type: none"><li>●</li><li>●</li><li>●</li></ul> |
| Brief overview of the content                                                                                                                                         |                                                                       |
| Resources used                                                                                                                                                        |                                                                       |

|                                       |  |
|---------------------------------------|--|
|                                       |  |
| Equipment / Resources needed          |  |
| Handouts / resources provided         |  |
| Other relevant information or queries |  |

## **PARENTS ACCEPTABLE USE POLICY**



### **St Andrew's CEVA Primary School Parents Acceptable Use Policy**

#### **Background & Rationale**

St. Andrew's Church of England Primary School is committed to providing a thriving Christian environment through the I ASPIRE values. These reflect the Christian ethos of our school and ensure that everyone feels safe, valued and supported so that all individuals can reach their highest goals and are encouraged to engage in lifelong learning. Our vision statement "*With God all things are possible*" (Matthew 19:26) is at the core of our values and is used to inspire everyone to be open to all possibilities and have a positive attitude and outlook to life. Spiritual, moral and emotional development are central to the life of our school and this will be reinforced in the School's Acceptable Use Policy for parents where appropriate.

We ask all children, young people and adults involved in the life of St. Andrew's CEVA Primary School to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP which you have signed and discussed already. We tell your children that **they should not behave any differently when they are out of school or using their own device or home network**. What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school:

***"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."***

You can read St. Andrew's CEVA Primary School's full Online Safety Policy here, for more detail on our approach to online safety and links to other relevant policies. If you have any questions about this AUP or our approach to online safety, please speak to Headteacher Mrs Val Griffiths.

### **What am I agreeing to?**

1. I understand that St. Andrew's CEVA Primary School uses technology as part of the daily life of the school when it is appropriate to support the teaching, learning, smooth running of the school and to help prepare the children in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents / carers.
4. I will support the school's online safety policy and encourage my child to not joint any platform where they are below the minimum age.
5. The school sometimes uses images/videos of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
6. I understand that for my child to grow up safe online s/he will need positive input from school and home, so I will talk to my child about online safety and refer to the school's website for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screen time and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
7. I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings for all the main internet providers in the UK. There are also child-safe search engines e.g. [swiggle.co.uk](http://swiggle.co.uk) and YouTube Kids is an alternative to YouTube with age appropriate content.
9. I understand and support the commitments made by my child in the AUP which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
10. I can find out more about online safety at St. Andrew's CEVA Primary School by reading the full Online Safety Policy and can talk to DSLS Mrs. V Griffiths, Miss. M Davidson and Mrs. S Gentry if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

**I/we have read, understood and agreed to this policy,**

**Signature/s:** \_\_\_\_\_

**Name/s or parent / guardian:** \_\_\_\_\_

**Parent / guardian of:** \_\_\_\_\_

**Date:**

---