St Alban's CVA

Online Safety Policy

Date issued: September 2024

Date for review: September 2026

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

[Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Stuart Olivier.

All governors will:

Ensure that they have read and understand this policy

Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL, along with the Headteacher, take lead responsibility for online safety in school, in particular:

ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working together with the ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school child protection policy

Ensuring that any online safety incidents are logged on Edukey and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged on Edukey and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The ICT Manager – (Trust IT Department)

The ICT Manager:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Working with the DSL to ensure that any online safety incidents are logged on Edukey and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2) This is provided as an online form

Ensure that they have read, understood and agreed to the parent terms on acceptable use of the school's ICT systems and internet. (appendices 1 and 2) This is provided as an online form

Monitor and supervise their child's online use of technology outside of school

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The academy will raise parents' awareness of internet safety in the newsletter or other communications home, and in information via our website. Parent / carer online safety workshops are offered regularly, led by an online safety specialist.

The academy engages with the I-vengers initiative which empowers a team of pupils to lead and promote online safety across the school community. It also involves communication with parents and carers.

School strongly advise parents / carers to make use of parental controls and ensure they are set on all devices that their children can access at home. The link to the NSPCC advice and support with setting up Parent Controls is sent out to all parents. https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

We clearly express it is parents / carers responsibility to monitor and supervise their child's online use of technology, outside of school, to ensure their child's safety.

Following specialist advice, school encourage parents / carers to engage positively and appropriately with their child's online interactions as this can help to prevent cyberbullying and to help their child stay safe online.

We strongly advise that pupils of primary school age do not use the following apps. These apps often contain content, interactions, or features that are not suitable for children under the age of 12. It's essential for parents and guardians to monitor and regulate app usage, ensuring age-appropriate alternatives are available.

TikTok
- Contains content not suitable for young children.
- Potential privacy and security concerns.

Snapchat
- Features like Snap Map and disappearing messages pose privacy risks.
- Exposure to inappropriate content.

Instagram
- High risk of exposure to inappropriate content and online predators.
- Pressure to conform to social media standards.

Facebook
- Not designed for young children.
- Exposure to inappropriate content and privacy concerns.

WhatsApp
- Can expose children to unsolicited messages and inappropriate content.
- Not designed with children in mind.

YouTube (without parental controls)
- Risk of exposure to inappropriate videos and comments.
- Ads and content not always suitable for young audiences.

Kik
- Known for privacy issues and potential for misuse by predators.
- Inappropriate content and messaging features.

Omegle
- Promotes anonymous chatting, often leading to exposure to inappropriate content.
- High risk of encountering predators.

Discord
- Though popular for gaming, it can expose children to inappropriate content and online bullying.
- Not specifically designed for young children.

Houseparty
- Potential for unmonitored interactions with strangers.
- Privacy concerns and inappropriate content.

Twitch
- Live streaming content may not be moderated appropriately.
- Potential exposure to inappropriate language and behaviour.

Reddit
- Contains a wide range of unmoderated content, much of which is not suitable for children.
- Community-based forums that can include inappropriate discussions.

Stars
- Contains live streaming and video content that may not be appropriate for young audiences.
- Potential exposure to unmoderated interactions and inappropriate content.

We expect pupils **not to access** the applications named above.

Where primary age pupils are using apps and sites that enable communication, it is expected that parents and carers are monitoring and filtering their conversations and interactions either using parental control or supervision.

The academy uses a trust wide system called LightSpeed to filter and monitor online use on the academy site.

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Pupils are taught that they should report any incidents of bullying to a trusted adult at home and / or at school.

Details of the school's approach to prevent and address bullying, including cyberbullying, are set out in our Anti-bullying Policy. It details how the school will challenge, address and monitor bullying (including cyberbullying) incidents to ensure it doesn't continue. It states that all pupils will be supported, including the target, perpetrator and any witnesses.

If school is made aware of cyberbullying incidents that take place outside of school, we will inform parents of those directly involved and although we will heavily support the parents and the pupils, the expectation is that it is the responsibility of the parents to manage the incident with their child at home. School will provide advice and tips on dealing with cyberbullying to the parents / carers and will support the pupils and families to resolve negative feelings. School will also monitor and support the pupils in school and will deal appropriately with any impact of the cyberbullying that may transfer into school.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

The school Behaviour Policy indicates that the school can issue behaviour sanctions to pupils for off-site online misbehaviour if the behaviour affects the school in anyway and / or it poses a threat or causes harm to another pupil.

Cyberbullying, as well as Online Safety is taught through a variety of ways including the Personal Development and Computing Curriculum, missions undertaken by the academy I-vengers Team, engaging annually with Safer Internet Day activities and through external agencies providing workshops such as PCSO's and online safety experts.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the school Behaviour Policy and the Anti-Bullying Policy.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

The school makes use of the the Professional Online Safety Helpline, http://www.saferinternet.org.uk/about/helpline which is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or

Is identified in the school rules as a banned item for which a search can be carried out, and/or

Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.

Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

Cause harm, and/or

Undermine the safe environment of the school or disrupt teaching, and/or

Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

The DfE's latest guidance on searching, screening and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

By attending St Alban's CVA, it is expected that all pupils and parents agree to the acceptable use of the school's ICT systems and the internet (appendices 1 to 2).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 2.

8. Pupils using mobile devices in school

We advise that children of primary school age do not own a smart phone. Pupils are not permitted to use any type of mobile device, brought in from home, including smart watches, whilst on school grounds. If a child does bring a mobile phone into school, it must be for practical home life reasons only and it must be handed in to the school office on arrival and collected when leaving the school site.

In rare and exceptional circumstances, any use of mobile devices in school by pupils must be supervised by a member of staff and be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping the anti-virus and anti-spyware software enabled by the Trust ICT department
- Keeping operating systems up to date by installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Trust ICT department. .

All staff members must adhere to the Trust Code of Conduct.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL, or other appropriate staff, log behaviour and safeguarding issues related to online safety on Edukey.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Anti-Bullying Policy

Staff Code of Conduct

Data protection policy and privacy notices

Complaints procedure

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS (COMPLETED DURING COMPUTING SESSIONS IN SCHOOL)	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask an adult if I can do so before using them
• Only use websites that an adult has told me or allowed me to use
• Tell an adult immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell an adult straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers, name of the school I attend) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network if sked to do so
• Check with an adult before I print anything
• Log off or shut down a computer when I have finished using it
 	
I understand that school can issue behaviour sanctions for online misbehaviour, even if this takes place at home, if the misbehaviour affects the school in any way and / or poses a threat or causes harm to another pupil.
I am aware that the school will monitor the websites I visit at school and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS (COMPLETED DURING COMPUTING SESSIONS IN SCHOOL)

Parent/carer agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

I / We understand that it is our responsibility as parents / carers to monitor and supervise my / our child's online use outside of school.

I / We are aware that school strongly advise the use of parental controls and encourage parents / carers to engage positively and appropriately with our child's online interactions to help prevent cyberbullying and to ensure my / our child's safety online.

I/ We are aware that if incidents of cyberbullying related to my / our child occur outside of school, that we will be informed by school if they have been made aware and the expectation is that as parents / carers we manage the incident with my / our child. We are aware that school will support with this and in some cases, sanctions may be issued by school.

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS (COMPLETED DURING COMPUTING SESSIONS IN SCHOOL)	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when an adult is present, or with an adults permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address, telephone number and name of the school I attend to anyone without the permission of my teacher or parent/carer • Tell a member of staff immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with an adult • Use any inappropriate language when communicating online, including in emails • Send unkind messages or communicate in any way, using a device, in an unkind manner towards another person • Create, link to or post any material that is inappropriate, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline **If I bring a personal mobile phone or other personal electronic device, including a smart watch, into school:** • I will not use it at all whilst on school grounds, including during morning or after school clubs or other activities organised by the school (such as school trips) • I will hand it in to the school office immediately **I understand that school can issue behaviour sanctions for online misbehaviour, even if this takes place at home, if the misbehaviour affects the school in any way and / or poses a threat or causes harm to another pupil.** **I am aware that the school will monitor the websites I visit at school and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS (COMPLETED DURING COMPUTING SESSIONS IN SCHOOL)

Parent/carer's agreement:

I / We agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I / We understand that it is our responsibility as parents / carers to monitor and supervise my / our child's online use outside of school.

I / We are aware that school strongly advise the use of parental controls and encourage parents / carers to engage positively and appropriately with our child's online interactions to help prevent cyberbullying and to ensure my / our child's safety online.

I / We are aware that the school strongly advise that pupils of primary school age do not use specific apps that are named within the policy.

I/ We are aware that if incidents of cyberbullying related to my / our child occur outside of school, that we will be informed by school if they have been made aware and the expectation is that as parents / carers we manage the incident with my / our child. We are aware that school will support with this and in some cases, sanctions may be issued by school.