Online Safety Policy

Prepared by:	Daniel Bishop
Agreed by governing body:	Autumn 2024
Review date:	Autumn 2026
Signed	
Chair of Governors:	
Headteacher:	

CHASE BRIDGE PRIMARY SCHOOL

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Mike Dormer is the link Governor for Safeguarding including Online Safety

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (refer to appendices)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college 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) Brian Ostro and the DDSLs Amy Gray and Daniel Bishop are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 7) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 half termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 7) 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

This list is not intended to be exhaustive.

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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (refer to appendices), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by making a referral to the Safeguarding Team.
- Following the correct procedures by informing the DSL and School Business Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 7) 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'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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)

Parents/carers 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
- Chase Bridge school website

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. If appropriate, they will be expected to agree to the terms on acceptable use (refer to appendices).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 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 (KS) 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/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website https://www.chasebridge.richmond.sch.uk/online-safety . This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers 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. (See also the school behaviour policy.)

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.

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. Class teachers, and SLT via assemblies, will discuss cyber-bullying within their computing lessons and during class discussing when the need arises.

Our PSHE curriculum has a comprehensive coverage of online safety with topics covered in almost every half term.

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 makes information available to support parents and families with online safety via our website.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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.

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 and/or the 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 co-operation

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 DSL or headteacher 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/carer 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

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Chase Bridge recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Chase Bridge will treat any use of AI to bully pupils in line with our Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. **Please see Appendix below for our AI policy and guidance.**

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Year 5 and 6 pupils may bring mobile devices (but they must not be smartphones) into school if their parents provide authorisation for them to walk to and from school unaccompanied. Pupils are not permitted to use their mobile devices whilst they are on the premises. Parents must seek school authorisation should they wish for their child to bring in a mobile device and must be in line with the acceptable use agreement (see appendix 6).

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 Fcharacters, 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
- Installing anti-virus and anti-spyware software
- To ensure the device is returned to the school for the latest security updates to be installed.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

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 School Business Manager.

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 policies on Behaviour and Acceptable Use. 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 that 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 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 logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 7.

This policy will be reviewed every year by the headteacher . At every review, the policy will be shared with the governing board. The review (such as the one available here) 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
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement

THE GUIDANCE AND RULES IN THIS AGREEMENT WILL BE DELIVERED IN LESSONS TO TEACH EYFS & KS1 PUPILS ON INTERNET SAFETY ALONG WITH SAFE AND RESPONSIBLE USE OF IT DEVICES.

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher if I can do so before using them
- Only use websites and apps that a teacher has told me or allowed me to use
- Tell my teacher immediately if:
    - I select a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset, worry 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 a teacher 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. I can only share my password with my parents.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network following my teacher's instructions
- Log off or shut down a computer when I have finished using it or to ask for help from my teacher
- I understand that the teachers will check how I use computers and tablets at school to make sure that I am following these rules and keeping myself safe.
- I also understand that it is important to follow these rules at home when I am doing my school homework.

Appendix 2: KS2 acceptable use agreement

THE GUIDANCE AND RULES IN THIS AGREEMENT WILL BE DELIVERED IN LESSONS TO TEACH KS2 PUPILS ON INTERNET SAFETY ALONG WITH SAFE AND RESPONSIBLE USE OF IT DEVICES.

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 school work and other activities to learn.
- Only use them when a teacher is present, or with a teacher's permission. At home, I will only use the websites for home learning after speaking with my parent/carer.
- 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 or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or trusted adult) immediately if I find any material which might upset, worry or harm me or others. 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.
- Not 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. I know anything I do can be shared and might stay online forever.
- I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, and report any bad behaviour to my teacher or parent/carer, at school and at home.
- Always log off or shut down a computer when I've finished working on it.

I will not:

- Attempt to 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.
- Use any inappropriate language when communicating with my teachers when using Seesaw.
- Create, link to or post any material that is inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I understand that the teachers will check how I use computers and tablets at school to make sure that I am following these rules and keeping myself safe.
- I also understand that it is also important to follow these rules at home when I am doing my school homework.

Appendix 3: Acceptable use policy - Staff

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF
What is an AUP? We ask all pupils and members of staff at Chase Bridge to sign an Acceptable Use* Policy (AUP), which outlines 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).
Why do we need an AUP? All staff (including support 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 as detailed in the full Online Safety Policy.
Where can I find out more? All staff, governors and volunteers should read Chase Bridge's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Child Protection and Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to a member of the Senior Leadership Team.

What am I agreeing to?

1. I have read and understood Chase Bridge's 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. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand 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 (if by a child) or Headteacher (if by an adult).
3. **During remote learning:**
    - **I will not behave any differently** towards pupils compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, 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 personal login for remote teaching** or set up any system on behalf of the school without SLT approval
    - **I will not take secret recordings or screenshots** of myself or pupils during live online sessions.
    - **I will conduct any online sessions in a professional environment** as if I am in school.This means I will be correctly dressed and in a suitable environment The camera view will not include any personal information or inappropriate objects.
    - **I will complete the issue log for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of pupils.
    - I understand that in 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.
4. I understand the responsibilities listed for 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.
5. 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 (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
6. 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.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF

7. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) 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 to the headteacher.
8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in the school's Online Safety Policy.
9. 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.
10. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the school's School Business Manager if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
11. I will not store school-related data on personal devices,storage or cloud platforms. I will only use school approved licensed software, respecting licensing, intellectual property and observe copyright rules at all times.
12. 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.
13. I will not bring my own IT devices to school without seeking prior SLT approval.
14. I will ensure any images taken of staff and pupils for school related purposes are in line with the school's current image consent list.
15. I will not 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.
16. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action and where appropriate,referral to the relevant authorities.

Please complete the provided Google Form to confirm your agreement to this AUP.

Appendix 4: IT user agreement - governors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR GOVERNORS
Governors should familiarise themselves with the following school policies: 1. Data Protection 2. Online Safety 3. Data Retention Policy Governors should be mindful of the **7 principles** of GDPR and the Data Protection Act: 1. Keep information secure 2. Only store data for as long as you need or are legally required to do so 3. Only use the data required to do your job 4. Only use data for the purpose specified 5. Ensure accuracy of data 6. Handle data transparently 7. Accountability - you need to justify why you have acted as you have
Practical guide for governors: 1. Governing Body documentation is stored electronically on the shared portal (Governor Hub or Governor Google Shared Drive). Any information downloaded from the shared portal onto a personal device should be deleted upon the completion of the task, including from the temporary internet files. 2. School email addresses should be used for school business. This prevents subject access requests to personal email accounts and facilitates compliance with any email retention period. Please note, that this email address can be monitored by appropriate individuals if there is due cause. 3. Email conversations should be professional at all times. Email messages are required to be disclosed in legal proceedings or in response to Subject Access requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, therefore do not write anything you would not want to read by others. 4. When using personal devices please ensure that the device has anti-virus in place and has been updated to limit potential vulnerabilities. The school appreciates that others may use the personal devices you access the system with however please ensure that you are the only person who can access your user account and that you understand that anything undertaken while you are logged in, will be considered done by you. 5. Governors must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals should be encrypted so that the information is only accessible by the intended recipient. The use of Governor Hub and/or Governor Google Shared Drive is recommended for sharing such information. 6. If Governors receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. 7. The school via the School Business Manager, should be informed of any confirmed or potential data breaches without undue delay to allow it to react and mitigate the impact. 8. I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'. 9. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies. 10. I understand that failure to comply with this agreement could lead to disciplinary action.

Appendix 5: Acceptable Use Agreement - Volunteers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR VOLUNTEERS

When using the school's ICT systems and accessing the internet in school, I will not:

1. Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
2. Use them in any way which could harm the school's reputation
3. Attempt to access social networking sites or chat rooms
4. Use any improper language when communicating online, including in emails or other messaging services
5. Share any school issued usernames and passwords with others or log in to the school's network using someone else's details
6. Use a personal mobile device whilst on the school site and especially not in the company of pupils
7. Take photographs or videos of pupil or staff
8. Share confidential information about the school, its pupils or staff, or other members of the community
9. Access, modify or share data I'm not authorised to access, modify or share
10. Promote private businesses

All volunteers who have access to school devices or IT infrastructure are required to read and provide an online acknowledgement of the school's Volunteer IT Acceptable Use Policy.

Appendix 6: Year 5 & 6 pupil mobile phone acceptable use policy

PUPIL MOBILE PHONE ACCEPTABLE USE POLICY - YEARS 5 AND 6 ONLY

Pupil Mobile Phone Acceptable Use Agreement

The curriculum in year 6 supports the children's gradual transition to secondary school. One element of this is the use of mobile phones. In the final year **children in year 6 are allowed to bring a basic, non-smart technology 'feature' phone** with them to school. 'Smart' technology devices (such as iPhones) are not permitted.

GPS Trackers

As a school, we strongly discourage the use of tracking devices with children of any age. However, we appreciate that some parents may have concerns once their child reaches an age to walk to/from school independently. If you do decide to provide your child (years 5 & 6) with a GPS tracking device (such as AngelSense or Gabb Watch), these will be treated in the same way as a mobile phone.

Bluetooth tracking systems (such as AirTag, Galaxy SmartTag2 and Tile) are not permitted in school. Their presence can cause false stalking alerts and make it difficult for the school to effectively safeguard all children and staff.
No form of GPS or Bluetooth tracking device is permitted on school excursions.

To promote safe and appropriate use of their mobile phones, we have created an Acceptable Use Policy which establishes clear and robust guidelines. This is to balance the risks and benefits as well as clarify the shared responsibility between home and school so that we can jointly protect and educate our children.

Pupils and their parents/carers must read, understand and sign this acceptable use policy before pupils are given permission to bring mobile phones to school. You may also want to read our Pupil Use of Mobile Phones and Smart Technology Policy on our school website.

It is the responsibility of pupils who bring mobile phones to school to abide by the guidelines outlined in this document; the decision to allow a mobile phone to be brought to school must be made by parents/carers with the agreement of the school.
Infringements of this policy may result in the confiscation or a ban on bringing a phone to school.

What we do:

- Phones are clearly labelled with the pupil's name.
- Phones are turned off and kept in bags before entering the school site.
- Phones should remain in pupils' bags until they go to class in the morning.
- Once the pupils go to class, the phones are given to the teacher. (Phones will be locked away until the end of the day.)
- Phones are given back at the end of the day from the class. If they have been at a club or similar after school activity they are collected from the school office.
- Phones can be turned on again at the end of the day once off the school site.
- Pupils should promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media.

Reminders:

- Mobile phones are not to be used on school site in any capacity by a pupil.
- Pupils should not gather around the school gates before or after school with their mobile phones out.
- The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.
- To reduce the risk of theft, pupils who carry mobile phones with them before and after school are advised to keep them well concealed and not 'advertise' they have them.
- Pupils must not share other's images or details without permission and not post or pass on negative, threatening or violent comments. It is a criminal offence to use a mobile phone to menace, harass or offend another person.

I/we have read, understood and agreed to this Mobile Phone Acceptable Use Agreement

Name/s of parent/carer: _____ Signature: _____

Name of pupil: _____ Signature: _____

Phone number of pupil's device: _____ Date: _____

Appendix 7: Online safety incident report log

Chase Bridge Serious Incident Form			
Date of incident		**Staff logging incident**	
Staff logging the incident must show this completed form to SLT and class teacher(s) and obtain their signatures at the back of this form			

When	Location	Type
before school	classroom	verbal
class time	corridor	physical
break/lunch	playground	continuous low-level disruption
after school	toilets	continuous defiance of adult instructions
out of school hours	clubs before/after school	theft
	off site	damage to property
	other	possession of dangerous object
		IT / E-Safety
		inappropriate sexual behaviour
		problematic sexual behaviour
		abusive sexual behaviour
		violent sexual behaviour
		other

Offender's possible motivation	racism	discrimination	games disagreement	other disagreement	unprovoked

Identify the victims and offenders with a V or O, as well as year, class and gender. (Note: there might only be offenders.)				
Name:	V / O	Year:	Class:	Gender: M / F
Name:	V / O	Year:	Class:	Gender: M / F

Name:	V / O	Year:	Class:	Gender: M / F
Name:	V / O	Year:	Class:	Gender: M / F
Name:	V / O	Year:	Class:	Gender: M / F

Give a brief summary of the incident. • Include **statements** from victim(s), offender(s) and eyewitnesses where necessary. • Speak to the victim/offender **separately** where necessary. • Indicate if **positive handling** was used.

Signatures			
SLT signature:		Teacher signature:	

SLT to complete	
Bullying is defined as repetitive, intentional harming of a person or group by another person or group, where the relationship involves an imbalance of power.	**Was this a bullying incident?** Yes / No

SLT to complete		
Response by school to incident		
Contact parents	School sanctions	Restorative conversation
SLT involvement	SENDCo involvement	External agency involvement
Suspension	Exclusion	Police
Positive handling		

Updated 20.09.2023

Appendix 1: AI Policy and Guidance

As technology evolves, including the use of Artificial Intelligence (AI) tools, it is essential that all school staff adhere to the following guidelines to ensure compliance with Data Protection regulations, safeguarding policies, and responsible ICT use. This addendum aligns with UK GDPR requirements and Chase Bridge Primary School's data protection policies.

Data Protection & GDPR Compliance

- Free AI tools may process and store data using global infrastructure that falls outside UK GDPR jurisdiction.
- Submitting any Personally Identifiable Information (PII), sensitive school data, or identifiable student/staff content can result in data protection breaches.
- Always anonymise any data before entering it into any AI tool or external platform.

Public Domain Risk

- Content entered into free AI platforms may be used to train future models, meaning that any submitted data—intended or accidental—could become part of a public dataset.
- Avoid entering confidential, sensitive, or proprietary school information.

Accountability & Safeguarding

- Staff must use AI tools responsibly and not rely solely on AI-generated content without verification.
- Misuse of AI tools, including generating inappropriate content, is strictly prohibited.
- The school has no control over external AI tools; therefore, all staff must exercise caution when using such platforms and data protection should drive all decisions.

Approval & Oversight

- ChatGPT is the preferred provider for AI usage within the school.
- Any other AI tools must be signed off by the Headteacher and DPO before use on the school site.
- Before using AI tools, staff must seek approval from the Headteacher or Data Protection Officer (DPO).
- If approved, the following minimum principles must be followed:

1. **Anonymise Data** – Do not input names, email addresses, UPNs, or any identifiable personal details.
2. **Avoid Confidential Content** – If the information feels private, do not enter it.
3. **Assume Public Exposure** – Treat AI tools as public spaces where data might be stored or accessed.
4. **Verify Accuracy** – AI-generated content must be reviewed for accuracy, bias, and appropriateness before use.
5. **Do Not Upload Documents** – Avoid sharing internal, sensitive, or protected school documents.