ALLEYN COURT PREPARATORY SCHOOL

Inc EYFS

Online-Safety Policy

COMPILED BY: P. Hart **UPDATED BY: D. Lewington**

VERSION 5 – September 2024 **DATE FOR NEXT REVIEW: September 2026**

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- 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, mobile and smart technology including electronic devices with imaging and sharing capabilities (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
- Relationship Education (Primary)
- 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.

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Chair of Trustees is responsible for online safety and will co-ordinate 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 Board of Trustees should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Board of Trustees 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 the 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 trustees will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- 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 (DSL)

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 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 Board of Trustees to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead, along with the Head of Computing, on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Headteacher and Head of Computing to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Head of Computing 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 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and Board of Trustees
- Undertaking annual risk assessments with Head of Computing 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 Head of Computing

The Head of Computing 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 monthly 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 5) 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL and Head of Computing are 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 emailing the DSL and Head of Computing.
- Following the correct procedures by emailing their request to Head of Computing 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 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the 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
- Parent resource sheet – Childnet

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 (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety, including the use of social media, as part of the Computing and PSHE curriculum and in other subjects where relevant and appropriate. Four areas of risk will be appropriately covered according to the area being taught and the age and stage of the children. These are content, contact, conduct and commerce. There will also be specific reminders in the first Computing lesson of every term.

The teaching of online safety forms part of children learning about their responsibilities to safeguarding themselves, e.g. what part they play in keeping themselves safe. As with all teaching and learning, all lessons should be adapted so the content is appropriate for the learners being taught. An overview of when online safety teaching occurs across the school can be found in (appendix 6).

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
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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. This policy will also be shared with parents/carers.

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 and Anti-Bullying 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. Form teachers will discuss cyber- bullying with their tutor groups, usually within the PSHE curriculum. Subject teachers may also cover this, when appropriate, within their lessons.

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/leaflets on cyber-bullying to parents/carers so 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 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 (as set out in your Behaviour Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils
- Is identified in the school rules as a banned item for which a search can be carried out
- 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 Senior Leadership Team
- 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
- Undermine the safe environment of the school or disrupt teaching
- Commit an offence

If inappropriate material is found on the device, it is up to the Senior Leadership Team/DSL 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 Headteacher) 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.

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.

Alleyn Court 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Alleyn Court will treat any use of AI to bully pupils in line with our anti-bullying/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.

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, trustees 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

Children are not permitted to use personal mobile phones within school or on any school activity or trip. In exceptional circumstances and with the express permission and approval of the Headmaster, they may be kept in a named bag at the School Office during the school day for emergency use when travelling to and from school only. Mobile phones will not be taken on school trips. Failure to adhere to this rule permits staff to confiscate a phone if a child has it in their possession at school. Any breech of the above may lead to disciplinary action in line with the school good behaviour policy, which may result in the confiscation of their device.

Children throughout the school will not be allowed to wear smart watches, Fitbits, or similar digital devices.

9. Members of staff and mobile technology

Personal mobile phones/ smart watches should only be used during the school day to take pictures of specific activities which will be used to promote the school through the school's social media platforms, on the website or displays. Once the images have been transferred to the school's picture server, they must be deleted as soon as is practicable. Staff Mobile phones/ smart watches need to be kept on silent and in the classroom store cupboard except if being used as stated above or there is an emergency where the school office or emergency services need to be called instantly.

In the EYFS personal mobile phones and other devices with imaging and sharing capabilities cannot be in any classroom and must kept in designated cupboards. A smart watch without camera function may be worn but all access to the internet must be disabled and emails, text messages or any notifications must not be received. Smart watches may only be used as a watch and fitness tracker.

SLT are expected to carry mobile phones on them, but not to use them without due cause.

Any breech of the above may lead to disciplinary action.

All staff members using work devices outside of school 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

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 Head of Computing.

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 disciplinary procedures / 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, 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, threatening, 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 and 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.

Trustees 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.

If you become aware of a breach of this policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it in line with the Whistleblowing Policy…**See It, Say It, Sort It.** Reports will be treated in confidence as far as is possible.

12. Monitoring arrangements

The Head of Computing and DSL log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Board of Trustees. 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.

Our filtering system is E2BN Protex – setup and controlled by E2BN. This is monitored by the schools Head of Computing and representatives from 'Croft' our Technician support company who manage the school's server.

The school's cyber security is provided by Sophos Anti-Virus, alerts and updates are completed by our Head of Computing or a 'Croft' technician.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Whistleblowing policy
- Behaviour policy
- Staff disciplinary procedures
- Privacy Notice
- Complaints procedure
- ICT and internet acceptable agreement

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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 or adult if I can do so before using them
• Only use websites that a teacher or adult 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 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
• 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
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
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.	
Signed (parent/carer):	**Date:**

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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 a teacher is present, or with a teacher's 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 or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that 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 a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise 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 agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/trustee/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • 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) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Head of Computing know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

Alleyn Court IT Dept. Online Monitoring Log					
Date	Type	Reported by	Person Involved	Details	Action(s)

Appendix 6: Online safety curriculum over view

Year Group	Term	Topic - *Theme (Relationships Education, RSE)*
EYFS – Reception	Autumn	- Ways to communicate online - Use of Tapestry - Sharing of passwords - Who is trustworthy
EYFS – Reception	Spring	- Know the internet can be used to find out information on line - Types of digital devices that can be used to access information on line
EYFS – Reception	Summer	- Whom to tell if they see something online that makes them feel happy/unhappy, excited/worried or scared - Ways people can be unkind online - Rules about sharing personal data (name, age, birthday, address
Year 1	Autumn	**Keeping safe** - basic rules for keeping safe online, - whom to tell if they see something online that makes them feel unhappy, worried, or scared
Year 1	Spring	**Media literacy and Digital resilience** - how and why people use the internet - the benefits of using the internet and digital devices - how people find things out and communicate safely with others online
Year 1	Summer	
Year 2	Autumn	**Safe relationships** - how to recognise hurtful behaviour, including online - what to do and whom to tell if they see or experience hurtful behaviour, including online
Year 2	Spring	**Media literacy and Digital resilience** - to recognise the purpose and value of the internet in everyday life - to recognise that some content on the internet is factual and some is for entertainment e.g. news, games, videos - that information online might not always be true
Year 2	Summer	**Keeping safe** - to identify potential unsafe situations, who is responsible for keeping them safe in these situations, and steps they can take to avoid or remove themselves from danger
Year 3	Autumn	**Safe relationships** - What is appropriate to share with friends, classmates, family and wider social groups including online **(consent)** - about what privacy and personal boundaries are, including online - basic strategies to help keep themselves safe online e.g. passwords, using trusted sites and adult supervision

		- about bullying online, and the similarities and differences to face-to-face bullying - what to do and whom to tell if they see or experience bullying or hurtful behaviour
Year 3	Spring	**Media literacy and Digital resilience** - how the internet can be used positively for leisure, for school and for work - to recognise that images and information online can be altered or adapted and the reasons for why this happens - strategies to recognise whether something they see online is true or accurate - to evaluate whether a game is suitable to play or a website is appropriate for their age-group - to make safe, reliable choices from search results - how to report something seen or experienced online that concerns them e.g. images or content that worry them, unkind or inappropriate communication
Year 3	Summer	**Respecting ourselves and others** - how to model respectful behaviour in different situations e.g. at home, at school, online **(consent)**
Year 4	Autumn	**Families and friendships** - about the features of positive healthy friendships such as mutual respect, trust and sharing interests including online **(consent)** - how to communicate respectfully with friends when using digital devices - how knowing someone online differs from knowing someone face to face and that there are risks in communicating with someone they don't know - what to do or whom to tell if they are worried about any contact online **Respecting ourselves and others** - how to model respectful behaviour in different situations e.g. at home, at school, online
Year 4	Spring	**Safe relationships** - What is appropriate to share with friends, classmates, family and wider social groups including online - how to respond safely & appropriately to adults they may not encounter (in all contexts including online) whom they do not know - about what privacy and personal boundaries are, including online - basic strategies to help keep themselves safe online e.g. passwords, using trusted sites and adult supervision - about bullying online, and the similarities and differences to face-to-face bullying - what to do and whom to tell if they see or experience bullying or hurtful behaviour
Year 4	Summer	**Media literacy and Digital resilience** - that everything shared online has a digital footprint - that organisations can use personal information to encourage people to buy things - to recognise what online adverts look like - to compare content shared for factual purposes and for advertising - that search results are ordered based on the popularity of the website and that this can affect what information people access
Year 5	Autumn	**Families and friendships** - the impact of the need for peer approval in different situations, including online - how to recognise if a friendship is making them feel unsafe, worried, or uncomfortable including online - when and how to seek support in relation to friendships including online

		Safe relationships - whom to tell if they are concerned about unwanted physical contact or general personal safety, including online
Year 5	Spring	**Media literacy and Digital resilience** - to identify different types of media and their different purposes e.g. to entertain, inform, persuade or advertise - basic strategies to assess whether content online (e.g. research, news, reviews, blogs) is based on fact, opinion, or is biased - that some media and online content promote stereotypes - how to assess which search results are more reliable than others - to recognise unsafe or suspicious content online - how devices store and share information
Year 5	Summer	**Respecting ourselves and others** - to identify online bullying and discrimination of groups or individuals e.g. trolling and harassment - how to respond if they witness or experience hurtful behaviour or bullying, including online (e.g. teasing, name-calling, bullying, trolling, harassment or deliberate excluding of others) - how to report concerns and seek help if worried or uncomfortable about someone's behaviour, including online
Year 6	Autumn	**Safe relationships** - strategies to respond to pressure from friends including online - how to get advice and report concerns about personal safety, including online **Physical health and Mental wellbeing** - how balancing time online with other activities helps to maintain their health and wellbeing - strategies to manage time spent online and foster positive habits e.g. switching phone off at night - what to do and whom to tell if they are frightened or worried about something they have seen online
Year 6	Spring	**Media literacy and Digital resilience** - about the benefits of safe internet use e.g. learning, connecting and communicating - how and why images online might be manipulated, altered, or faked - how to recognise when images might have been altered - why people choose to communicate through social media and some of the risks and challenges of doing so - that social media sites have age restrictions and regulations for use - the reasons why some media and online content is not appropriate for children - how online content can be designed to manipulate people's emotions and encourage them to read or share things - about sharing things online, including rules and laws relating to this (consent) - how to recognise what is appropriate to share online - how to report inappropriate online content or contact **Respecting ourselves and others** - ways to participate effectively in discussions online and manage conflict or disagreements
Year 6	Summer	**Keeping safe** - how to protect personal information online - to identify potential risks of personal information being misused - strategies for dealing with requests for personal information or images of themselves

		- to identify types of images that are appropriate to share- with others and those which might not be appropriate- that images or text can be quickly shared with others, even when only sent to one person, and what the impact of this might be - what to do if they take, share or come across an image which may upset, hurt or embarrass them or others - how to report the misuse of personal information or sharing of upsetting content/ images online - about the different age rating systems for social media, T.V, films, games and online gaming - why age restrictions are important and how they help people make safe decisions about what to watch, use or play