ALLEYN COURT PREPARATORY SCHOOL

Inc EYFS

e-Safety Guidance

Mobile Phones

Safe Use of Images

Staff I.T. Guidance

COMPILED BY: Paula Hart
VERSION 4 – October '21

UPDATED BY: Paula Hart
DATE FOR NEXT REVIEW: July '23

Contents

At Alleyn Court Preparatory School we are committed to ensuring that our whole school community is able to operate with safety and confidence whenever and wherever they use the Internet or mobile digital technologies.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

What is e-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones/ tablets/ smart phones/ laptops etc as well as collaboration tools and personal publishing. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Links with other policies

The school's e-safety policy operates in conjunction with other policies including;

Child Protection and Safeguarding Policy
Good Behaviour Policy
Anti- Bullying Policy
Curriculum Policy
Data Protection Policy and Privacy notice
Complaints procedure
Staff disciplinary procedure
Data Protection

Aims

Our school aims to;

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation and Teaching online safety in school. It also refers to the Department'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.

This policy also takes into account the EYFS Statutory Framework 2021 and our computing program of study (see page 5).

Roles and responsibilities

The board of trustees

The board of trustees has overall responsibility for monitoring this policy and holding the headmaster to account for its implementation.

The trustee responsible for e-safety, Dr J Collis, will meet regularly with appropriate staff to discuss online safety, and monitor the online safety log as provided by the designated safeguarding lead (DSL).

All trustees will:

- Ensure that they have read and understand this policy

The headmaster (Mr Snow)

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

The designated safeguarding lead (Mrs Hart – Pastoral Deputy Head)

Details of the school's designated safeguarding lead (DSL) [and deputies] are set out in our child protection and safeguarding policy.

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

- Supporting the headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headmaster, Head of Computing and ICT, and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (as other child protection concerns) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged (in the Bullying record) and dealt with appropriately in line with the school good 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 headmaster
- This list is not intended to be exhaustive.

The Head of Computing and ICT (Mr Velleman)

The Head of Computing and ICT is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Ensuring anti-virus, back up and server integrity are checked on every visit by our IT support company (Badger) on their bi weekly, term time visits, including notification of anti-virus alerts.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (as other child protection concerns) with the DSL 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 good behaviour policy (reporting to the DSL)

This list is not intended to be exhaustive.

Social Media and website (Mr Smith)

- Will ensure content is current and appropriate
- Advise/ encourage staff to contribute to social media sites and monitor them

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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 (appendix 2)
- Working with the DSL to ensure that any online safety incidents are logged (as other child protection concerns) 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 (reporting to the DSL).

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headmaster of any concerns or queries regarding this policy
- Read through, with their child, the terms of acceptable use of the school's ICT systems and internet (appendix 2)
- Consult with the school if they have concerns about their children's use of technology
- Promote positive online safety and model safe, responsible positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, trustees, contractors, pupils or other parents/carers. If there is a concern about the school parents are urged to contact the school directly and in private to resolve the matter

The school will maintain a list of e-safety resources for parents/carers (see Information and support page 11). Parents have access to CEOPs on the school website (at the bottom of the menu page).

Educating pupils about online safety

Pupils will be taught about online safety, including the use of social media, as part of the ICT, 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 (4C's). There will also be specific reminders in the first ICT 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 1.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters, newsletters and in information via our website. An annual parent information evening is also organised. This policy will also be shared with parents.

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

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

Cyber-bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school good behaviour policy and anti-bullying policy.)

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 also cover this, when appropriate, within their lessons.

All staff, trustees and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section on Training for more detail, page 9).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Good 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees are expected to read the acceptable use of the school's ICT systems and the internet (appendices 2 and 3).

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 and trustees (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use of the school's ICT systems and internet in appendices 2 and 3.

Children and mobile technology

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 in the Pre-Prep are not allowed to wear smart watches.

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 Pre-Prep and EYFS mobile phones and smart watches cannot be in any classroom and must kept in designated cupboards.
SLT are expected to carry mobile phones on them, but not to use them without due cause. Further guidance can be found on page 11.
Any breech of the above may lead to disciplinary action.

See page 13 for more information regarding staff and the use of technology.

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 the Good 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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, if this is in September this will happen as part of the safeguarding training all staff have at the beginning of each school year.

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).

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 about 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety (as other child protection concerns).

This policy will be reviewed biannually by the DSL and updated before then, should it be necessary. At every review, the policy will be shared with the board of trustees.

Filtering and security

Our filtering system is E2BN Protex – setup and controlled by E2BN. This is monitored by the schools Head of Computing and ICT, Mr Velleman, and representatives from 'Badger' 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 Mr Velleman or a 'Badger' technician.

The school's wireless network is encrypted to prevent unauthorised access.

When dealing with the Internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps have been taken.

Published Content and the School Web Site

The contact details on the school website are the school address, e-mail and telephone number. Staff and pupils' personal contact information is not published.
The school maintains a current record of all pupils whose photographs or work may not be published. On admission, parents are requested to complete the appropriate form.
Photographs that include pupils are carefully selected and appropriate for the context. Pupils' full names are not used anywhere on the website in association with photographs.

General Data Protection Regulation (GDPR)

In accordance with the Data Protection Act 1998, users are not allowed to access other users' personal files and folders, including School e-mail. The exception to this being the Head of ICT who can gain access when just cause has been established.

Information and support

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.pshe-association.org.uk
www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

http://www.childnet.com/parents-and-carers/hot-topics

Staff personal mobile phone/ device guidance

- Staff use of their personal mobile phones/ smart watches/ device during their working school day should be:
  - Outside of their contracted hours with the pupils
  - Discreet and appropriate e.g. Not in the presence of pupils.

- Personal mobile phones/ smart watches should be switched to silent and left in a safe place during lesson times, unless they are being used to take pictures of events happening in the lesson. School will not take responsibility for items that are lost or stolen. Pre-Prep and EYFS must keep their mobile phones and smart watches out of the classroom in the designated cupboard.

- Staff should not contact pupils or parents from their personal mobile phone, or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil/ parent, a school telephone should be used, exceptions may only be for trips, sporting fixtures, off site activities or delayed pick-up after the school office has closed. In this case staff should ensure they use the 'no caller ID' option on their phones
- Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.

- With regard to personal camera mobile phones/ smart watches/ devices, a member of staff should only use their phone/ device to photograph a pupil(s) to take pictures for the school 'twitter' accounts, displays around school or in children's books, the school website or other social media platforms etc. Once photos have been used in this fashion they **must** be deleted from the phone.

- This guidance should be seen as safeguarding for members of staff and the school.

- For any extenuating circumstances, permission to use personal mobile phones must be sought from the Headmaster, Head of Pre-Prep or the Deputy Heads.

- In the event that misuse of a personal mobile phone/smart watch/ device is suspected, any member of the school's SLT may check an individual's mobile phone/ smart watch/ device for any inappropriate images.

- As an independent school, we will respond to any requests from the DBS for information we already hold that will not necessitate finding information from any additional sources.

- Mobile devices brought into school are entirely at the staff member, parents or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of such devices.

Safe use of Images Guidance

We recognise that photographs and video recordings for school and family use are an important record of a child's journey through the school. Most schools seek to use images to allow insight into the daily experiences of children and we offer that opportunity through sharing images on our website, in the school magazine and online, through Twitter. However, the potential misuse of images requires that everyone has a shared responsibility to ensure that individual and parental rights are respected, and that vulnerable individuals are protected from risk. The taking of photographs or videos at school events is not a breach of the Data Protection Act and is permitted by Alleyn Court Preparatory School.

All parents/carers are, however, reminded about their role in keeping every child safe by not publishing images online, particularly on social networking sites. ***This paragraph is read out or paraphrased at every school event where parents may wish to take photographs or videos.***

Parents and carers will not be permitted to take photographs, or video recordings during normal school routines (e.g. at the beginning, or end of the day, in classrooms, or whilst acting as a voluntary helper on a school visits), unless specifically requested to by a member of staff, or through application to the school office. Photographs taken for official use in school, or to be shared with a wider audience (either through the press or online), may be subject to the provisions of the Data Protection Act.

Permission from those with parental responsibility for a child is needed before photographs are taken for publication. Parents are asked to **complete a form on admission** to the school and records of children whose images must be protected are maintained by the office. It is **the responsibility of the member of staff** taking or publishing the photos to find out about children whose images should not be used. If parents disagree over consent, it will be treated that consent has not been given.

When images are recorded for school use and/or publication it is important that pupils are suitably dressed and care must be taken during PE lessons. All images should be screened by the photographer for acceptability and any image that could be used inappropriately should be deleted appropriately.

Staff should be aware that in terms of taking an image to give a sense of the activity, or the enjoyment of children in a setting, **images of groups** are frequently more appropriate than individual children, as are **images taken from behind** as this makes the children less identifiable. Images should also be inclusive, showing boys and girls from different backgrounds and abilities. In publications where the pictures have captions, it is good practice to only include first names, although local press will insist on publishing surnames. Schools may keep photographs and video recordings as evidence of children's learning and as a record of school events. Digital images are stored on servers, cloud-based storage and images taken on I-pods used specifically for that purpose. In the Pre-Prep and EYFS 'Tapestry' is used to record each child's progress and includes photographs. Parents can access their child's profile using a unique log on.

Staff in the Main School can use their own devices for taking pictures and should delete them as soon as possible after the images have been transferred to the pictures shared server. Parents used as official photographers, will be asked to hand the school the images taken on a memory stick, from which the school will copy the images and remove them. Parent helpers, whether in the classroom or on a school trip, **must not** take photos of the children. This must be made explicitly clear when parents are asked to help for a school activity.

Any suspicions concerning someone taking, or distributing images of children, should be taken to our Designated Safeguarding Officer (Mrs Paula Hart), the Headmaster, or the Police. (see the School Safeguarding Policy)

Use of Twitter

The school uses Twitter as a means of giving parents a better sense of what the daily experience of their child has been. We aim to afford parents an opportunity to engage in deeper conversation about something that happened in school, with their child and to engage parents more deeply into the Alleyn Court family. Details of the various accounts can be found below.

The Pre-Prep (EYFS) will release one photo Tweet a week, per class and about two prose-based tweets on various subjects.

The Upper School will Tweet within Year Groups and Subject Areas. There will also be a newsletter which may contain images. Most images will be posted within the school website in the relevant subject/year Group sections.

This guidance is subject to continuous development, as we are clearly in a period of significant change in respect to the taking, recording and sharing of images in an appropriate manner. The school does not wish to resort to a draconian approach but would rather work to secure guidance and procedure that adheres to our core values, developing **curious, courageous and compassionate** children, well-prepared to meet the demands of their extraordinary futures.

Staff Information Technology Guidance

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

Only access school IT systems using your own username and password. Do not share your username or password with anyone else.

Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

Do not attempt to install software on, or otherwise alter, school IT systems.

Do not use the school's IT systems in a way that breaches the principles of online behaviour set out below.

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.

Online behaviour

As a member of the school community you should follow these principles in all your online activities:

Ensure that your online communications, and any content you share online, are respectful of others.

Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism).

Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.

Do not access or share material that infringes copyright, and do not claim the work of others as your own.

Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

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

Work devices must be used solely for work activities.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy, Social Networking Policy, Mobile Phone Policy and Display Screen Equipment Policy

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety 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.

Appendix 1: 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

Appendix 2: acceptable use for pupils and parents

Acceptable use of the school’s ICT systems and internet: for pupils and parents/carers

When using the school’s ICT systems and accessing the internet in school, pupils will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school’s network using someone else’s details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

If pupils bring a personal mobile phone or other personal electronic device into school:

- Parents will first have sort permission from Mr Snow and will leave it in the school office with their name on the device.

Pupils know the school will monitor the websites they visit.

Pupils will immediately let a teacher or other member of staff know if they find any material which might upset, distress or harm them or others.

Pupils know they must always use the school’s ICT systems and internet responsibly.

Appendix 3: acceptable use for staff, trustees, volunteers and visitors

Acceptable use of the school’s ICT systems and the internet: for staff, trustees, volunteers and visitors

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, staff, trustees, volunteers and visitors will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which 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
- Share my password with others or log in to the school’s network using someone else’s details

They 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 their role.

They agree that the school will monitor the websites visited.

They 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.

They will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs them they have found any material which might upset, distress or harm them or others, and will also do so if they encounter any such material.

They will always use the school’s ICT systems and internet responsibly and ensure that pupils in their care do so too.