

ONLINE SAFETY POLICY

The 'School' refers to all staff and pupils in Abbot's Hill School, which includes the Early Years/Foundation Stage (EYFS), the Pre-Prep, Prep and Senior School.

The term 'parent' refers to those who have a parental responsibility for a child.

MONITORING AND REVIEW

Person Responsible	DSL
Reviewed by	DDSLs, Director of Technology
Approved by	Head
Frequency of Review	Annually
Date of Last Review	September 2023
Date of Next Review	September 2024

Contents

1. Introduction and Aims	3
2. Scope, legislation and guidance	4
3. Roles and responsibilities	5
4. Educating pupils about online safety	7
5. Educating parents/carers about online safety	9
6. Cyberbullying	9
7. Acceptable use of the internet in school	11
8. Pupils using mobile devices in school	12
9. Staff using work devices outside school	12
10. Social media	12
11. How the school will respond to issues of misuse	13
12. Training	13
13. Monitoring arrangements	15
14. Review	15
Appendix: Acceptable Use Agreements	16

This online safety policy is linked to our:

- o Child Protection and Safeguarding Policy
- o Promoting Positive Behaviour policy
- o Staff Disciplinary Procedures
- o Staff Code of Conduct and Safer Working Practice
- o Data Protection Policy and Privacy Notices
- o Image Authorisation Policy
- o Complaints Policy
- o ICT and Internet Acceptable Use Policies and Agreements
- o All these are available to staff and if appropriate to parents on request.

1. Introduction and Aims

It is the duty of Abbot's Hill School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks including, but not limited to, the risk of identity theft, bullying, harassment, grooming, exploitation, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. This policy acknowledges that online safety is as much about behaviour as it is about electronic security.

This policy, supported by the ICT Acceptable Use Policy for staff, pupils and visitors is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and deal with any infringements. Whilst exciting and beneficial, much IT, particularly online resources, are not consistently policed. All users must be aware of the range of risks associated with these internet technologies.

At Abbot's Hill, we understand the responsibility to educate our pupils on online safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas. Our school aims to:

- o Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- o Identify and support groups of pupils that are potentially at greater risk of harm online than others, including children with special educational needs.
- o 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')
- o Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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

- o **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- o **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
- o **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
- o **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Scope, legislation and guidance

This policy applies to all members of the school community, including staff, pupils, parents and visitors who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and support staff, governors and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the ICT Acceptable Use Policies cover both fixed and mobile internet devices provided by the school as well as any devices owned by pupils, staff or visitors that are brought onto school premises.

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#) (2023) and its advice for schools on:

- o [Teaching online safety in schools](#)
- o [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- o [Relationships and sex education](#)
- o [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 Governors

The Board of Governors is responsible for the approval of this policy and for reviewing its effectiveness. The Governor's Education committee will review this policy at least annually. The Safeguarding Governor liaises with the school about online safety.

3.2. The Head

The Head is responsible for the safety of members of the school community and this includes responsibility for online safety. The Head has delegated day-to-day responsibility to the Designated Safeguarding Leads (DSLs) and their deputies, who are supported by the Director of Technology and the Digital Strategy Group.

In particular, the Head and the Executive team must ensure that:

- Staff are adequately trained about online safety; and
- Staff are consistently implementing this policy; and
- Staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of online safety in connection to the school.

3.3. The Designated Safeguarding Lead

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

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

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head and Governors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead responsibility for implementing the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Director of Technology to make sure the appropriate systems and processes are in place
- Working with the Head, Director of Technology 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 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 Head and/or Governors
- 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 Director of Technology

Along with the Technology team, the Director of Technology is responsible for:

- Maintaining a safe technical infrastructure at school and keeping abreast of the rapid succession of technological developments
- The security of the school's computer systems and data and for training the school's teaching and support staff in the use of IT
- 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Enabling the monitoring of pupil and staff use of the internet and email, to ensure that any online safety incidents are reported effectively to the Safeguarding team and logged and dealt with appropriately in line with this policy
- Where any incidents of cyberbullying are identified, that these are passed to the Safeguarding team for action.

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:

- Accepting and following this policy and the ICT Acceptable Use Policies (the latter must be accepted before accessing the school's systems)
- Implementing these policies consistently
- Ensuring that pupils follow the school's terms on acceptable use (see appendix) and knowing what to do if acceptable use guidance is not adhered to
- Knowing that the DSLs are responsible for implementing the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by making an entry on CPOMS and alerting the DSLs
- Contacting the Director of Technology if they need to bypass the filtering and monitoring systems for educational purposes, with good reason
- 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

Abbot's Hill School believes that it is essential for parents to be fully involved with promoting e- safety both in and out of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it actively encourages parents to feel able to share any concerns with the school.

Parents/carers are expected to:

- Notify a member of staff or the Head 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

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](#)

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 (see appendix).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum at Abbot's Hill.

All schools have to teach:

- [Relationships education and health education](#) in our Pre-Prep and Prep School
- [Relationships and sex education and health education](#) in the Senior School

In **Pre-Prep**, 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 **Prep** 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 Prep school (Year 6)**, 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

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of Senior school (Year 11)**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- 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

- o How information and data is generated, collected, shared and used online
- o 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
- o 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, through a culture of talking about issues as they arise.

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

Pupils should be aware of the impacts of cyberbullying and know how to seek help if they are affected by these issues.

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.

Online safety will also be covered during parent education evenings and other events as relevant.

The school will let parents/carers know:

- o What systems the school uses to filter and monitor online use
- o 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 IT teaching team to seek advice and then they will feed through to relevant members of SLT/the safeguarding team.

6. Cyberbullying

6.1. Definition

Cyberbullying 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 Anti-Bullying policy and Positive behaviour policy).

6.2. Preventing and addressing cyber-bullying

To help prevent cyberbullying, 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. Abbot's Hill will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form tutors will discuss cyber-

bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Personal Development Education (PDE), and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyberbullying, Abbot's Hill will follow the processes set out in the school Anti-Bullying Policy and Promoting Positive 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 DSLs 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 Head, and any member of staff authorised to do so by the Head (usually the DSLs or DDSLs), 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 Head
- 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 the Head 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:

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

- o **Not** view the image
- o 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:

- o The DfE's latest guidance on [searching, screening and confiscation](#)
- o UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- o Our Promoting Positive Behaviour Policy

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

7. Acceptable use of the internet in school

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 (see appendix).

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.

The online filtering and monitoring software 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 the appendix.

Staff should not have their mobile phone out while in any areas with pupils unless absolutely necessary.

Images are not allowed to be taken of pupils on any personal devices. Phones are allowed to be used in emergencies but this must be shared with SLT.

For further details in EYFS, please see the related policies/processes.

8. Pupils using mobile devices in school

Pupils in Years 7-11 may bring mobile devices into school but are not permitted to use them during the school day. They are handed in to a relevant location when they arrive onsite. This is shared to staff at the beginning of the year and overseen by the HoYs.

Pupils in the Prep school must have written permission from their parents to have a phone. This is only granted if necessary. These are handed in at Main Reception when they arrive at school.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, spaces, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- 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 the appendix.

Work devices must be used for appropriate activities.

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

10. Social media

Expectations

- The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times

Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities

- Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct and staff Acceptable Use Agreement.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age
- The school will control pupil access to social media whilst using school-provided devices and systems on site and on a school device at home:
 - The use of social media during school hours for personal use is not permitted.
 - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary and/or removal of internet facilities
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

11. How the school will respond to issues of misuse

Abbot's Hill School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the relevant Safeguarding Children Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from external agencies.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies and procedures, in particular the Child Protection and Safeguarding Policy, Promoting Positive Behaviour Policy and Anti-Bullying 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 Policy and procedure and Staff Code of Conduct and Safe Working Practices policy. 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.

12. Training

All new staff members will receive training, as part of their induction, on Abbot's Hill's Online Safety Policy and Acceptable Use Policies.

All staff members will receive regular information and training throughout the academic year, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school procedures. A CPOMS entry must be completed by staff as soon as possible if any incident relating to online safety occurs.

These entries should be red-flagged as a child protection concern so that the Safeguarding team will be alerted, who will liaise further as needed.

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 do not 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 DDSs 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.

As appropriate, nominated Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. All Governors receive Safeguarding updates which include Online Safety matters.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

13. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety. This incident log is found on Teams and a summary of behaviour and actions arising is reported to Exec termly.

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

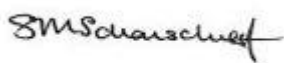
14. Review

This policy shall be reviewed annually, unless a major change merits earlier revision Last

Review: September 2023

Next Review: June 2024

This policy has been approved by:



Mrs Sharon Schanschieff

HEAD

Appendix: Acceptable Use Agreements

2023-24 ICT Acceptable Use Agreement: Prep

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. Pupils should sign a copy of the ICT Acceptable Use Agreement annually.

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes. All use is monitored and available to my teachers.
- I understand that the school's Online Safety Policy has been drawn up to protect all parties - the pupils, the staff, visitors and the school. It is available on the website and the Parent Portal.
- I will only use my school e-mail address when e-mailing from school.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe and ensure all my contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own/others' details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I may bring in my own device for reading from Year 5 in accordance with the Use of Personal

Device Agreement. This cannot be a mobile phone or iPod.

- I will not bring in memory pens/CD/DVDs into school unless I have permission.
- I will ensure that my online activity, both in school and outside school is in accordance with the law. I will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.

Remote Learning Guidelines

- I will respect the interactions and behave respectfully towards teachers and other pupils.
- I will be appropriately dressed for learning.
- I will not record or take photos of classmates or teachers during face-to-face sessions.
- I understand that when using Google Classroom and other applications provided by the school that my use may be monitored and logged and can be made available to my teachers.
- I will not use video conferencing when in my bedroom unless arrangements have been made with a member of Exec.
- I understand that these rules are designed to keep me safe and if they are not followed, school sanctions will be applied and my parents may be contacted.
- Only attend Google Meet between 8.15am and 4.30pm.
- I must leave Google Meet when instructed to by the teacher and before the teacher closes the meeting.
- I understand there must be a minimum of 3 pupils in any video conference unless arrangements have been made with a member of Exec.

I have read and understood the ICT Acceptable Use Agreement

I understand that these rules are designed to keep me safe and that the school's Online Safety Policy has been drawn up to protect all pupils, staff, visitors and the school. It is available on the website and My School Portal. I understand that if I don't follow this agreement, school sanctions will be applied and my parent/carer will be contacted.

I will ensure that my online activity, both in school and outside school is in accordance with the law. I will not cause my school, the staff, pupils or others distress or bring the school community into

disrepute, including through uploads of images, video, sounds or texts.

Network access will only be given to pupils that have signed this **ICT Annual Acceptable Use Agreement**.

Signature of pupil

Signature of parent

2024 - 2025 - ICT Acceptable Use Agreement – Senior Pupil

The Online Safety Policy has been drawn up to protect everyone: pupils, staff, visitors and the school itself. These rules help keep everyone safe and help us treat others fairly. This agreement applies to school and personal devices used anytime and anywhere.

- All users must ensure that all online activity is in accordance with the law.
- Activity that threatens the integrity of the school systems, or that attacks or corrupts other systems, is forbidden.
- Access must only be made via the authorised pupil login and password, which must not be made available to any other person.
- Users must not attempt to circumvent any filtering or monitoring systems.
- USB storage devices (pens/hard drives) are not permitted in school unless you have permission.
- Responsible use of devices is expected within school, on school buses and on school outings.
- School devices are filtered and monitored on and off-site. Including but not limited to: live viewing of screens, e-mails, chats, internet browsing history, user files.
- Internet sites and materials accessed must be appropriate to a pupil's education.
- Users will report inappropriate sites to a member of staff so that they can be blocked.
- Copyright of materials and intellectual property rights must be respected.
- The normal rules of social interaction apply to all forms of digital communication. Suitable language should be used, and anti-social behaviour, harassment, intimidation and bullying is forbidden.
- Use of social networking sites, chat rooms and instant messaging is not permitted on the school networks, except as explicitly authorised by the school. Posting anonymous messages and forwarding chain emails is forbidden.
- Images and recordings may only be taken within the school, or during school outings, with the permission of a member of staff (in accordance with our Image Authorisation Policy).

Mobile and Smart Devices

- Mobile and Smart devices (including all devices capable of recording) must be handed in to the Form Tutor at morning registration and collected from the library at 4.30pm.

- These devices should be switched off and kept out of sight between 8.15am and 4.30pm (unless permission granted by supervising teacher).
- Devices must not be brought into any examination room.

Nursery Visits:

- Mobile phones and personal devices are prohibited.
- The Nursery Manager will securely store devices for the duration of the visit.
- It must remain switched off until you leave the Nursery grounds.
- The school accepts no responsibility for lost or stolen devices. Parents are advised to ensure that their insurance provides appropriate cover.

Remote Learning Guidelines

- I will respect the interactions and behave respectfully towards teachers and other pupils.
- I will be appropriately dressed for learning.
- I will not record or take photos of classmates or teachers during face-to-face sessions.
- I understand that when using Google Classroom and other applications provided by the school that my use may be monitored and logged and can be made available to my teachers.
- I will not use video conferencing when in my bedroom unless arrangements have been made with a member of Exec.
- I understand that these rules are designed to keep me safe and if they are not followed, school sanctions will be applied and my parents may be contacted.
- Only attend Google Meet between 8.15am and 4.30pm.
- I must leave the Google Meet when instructed to by the teacher and before the teacher closes the meeting.
- I understand there must be a minimum of 3 pupils in any video conference unless arrangements have been made with a member of Exec.

I have read and understood the ICT Acceptable Use Agreement

I understand that these rules are designed to keep me safe and that the school's Online Safety Policy has been drawn up to protect whole school community.

I understand that if I don't act in accordance with this agreement, sanctions will be applied and my parent/carer may be contacted.

Signature of pupil

Signature of Parent