

E-safety and the use of ICT Policy

This policy refers to all of Chandlings Prep sections including EYFS

Technology has transformed the entire process of teaching and learning at Chandlings Prep. It is a crucial component of every academic subject, and is also taught as a subject in its own right (not in EYFS). Most of our classrooms are equipped with electronic whiteboards, projectors and computers. We have one Digital Learning suite in the school and Chromebooks and tablets are distributed for pupils to use, while supervised by a member of staff. Children in Prep each have a school managed chromebook for use in school and at home.

Where online research is necessary, our pupils are taught how to use the internet and to evaluate sources. The importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution, is taught. Some sites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, extremist or other propaganda.

Policy development, monitoring and review

This Online Safety Policy has been developed by the E-safety Coordinators and Online Safety Group made up of:

- Head of Year 3 and 4 and Head of Year 5 and 6
- The Head of Digital Learning
- Designated Safeguarding Lead
- Head of IT (Prep Schools) Radley Schools Group
- Trustee

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Responsibilities

Our E-safety Coordinators are The Head of Digital Learning and the Designated Safeguarding Lead

Responsibilities: Coordinators

Our E-safety Coordinators are the persons responsible to the Trustees for the day to day issues relating to e-safety. The E-safety Coordinators

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/documents
- Lead the Online Safety Group
- Ensure that all staff and trustees are aware of the procedures that need to be followed in the event of an e-safety incident and provide training and advice them
- Liaise with Radley Schools Group IT team

- Create a log of incidents via CPOMS to inform future e-safety developments immediately.
- Monitor the use of the internet through Securely and report inappropriate usage to the pastoral staff.
- Set up restrictions for use of school Chromebooks at home. There is a control on access after hours and during holidays via our filter system. Pupils cannot access their Chromebooks between 8pm and 6am.
- The DSL and Head of Digital Learning will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online.

Responsibilities: Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Responsibilities: Head

- The Head is responsible for ensuring the safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety is delegated to the e-safety coordinators
- The Head is responsible for ensuring that the E-safety Coordinators and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Responsibilities: Staff and Trustees

Teaching and Support Staff are responsible for ensuring that:

- All staff safeguard the welfare of children and refer any child protection concerns using the proper channels
- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix A)
- Online safety issues are embedded in all aspects of the curriculum and other activities
- They report any suspected misuse or problem to the E- Safety Coordinators
- Pupils understand and follow the acceptable use policies
- They embed e-safety issues in the curriculum and other school activities. The children's AUP actively promoted during Digital Learning lessons and when children are using Chromebooks

Responsibilities: Group IT Technician

The IT Technician is responsible for ensuring that:

- The school's IT infrastructure and data are secure and not open to misuse or malicious attack

- Users may only access the school's networks through a properly enforced password protection policy as outlined in this policy

Responsibilities: Online Safety Group

The Online Safety Group provides a consultative group with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the E-safety Coordinators with:

- the production/review/monitoring of the school online safety policy/documents.
- the production/review/monitoring of the annual school filtering and monitoring audit and requests for filtering changes.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision

Responsibilities: Students/Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of Chromebooks. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Responsibilities: Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the School and wider community, using officially sanctioned school mechanisms.

E-safety (Online Safety) Policy

The School Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the School and how they should use this understanding to help safeguard learners in the digital world
- describes how the School will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (to be described)
- is published on the School website.

Acceptable Use Agreements

All members of the school community are responsible for using the School IT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems. Pupil (KS1 and KS2) and Staff Acceptable Use Agreements are provided in Appendix A and Appendix B. Visitor and Parents Acceptable Use Agreements are in Appendix C and D.

The School believes that the activities listed below are inappropriate in a school context (**those in bold are illegal**) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, email, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images (illegal - The Protection of Children Act 1999)**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**

- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on IT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- Online gambling and non educational gaming

Reporting

The School will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- The Designated Safeguarding Lead, E-safety Coordinators and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart below), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Head, in which case the complaint is referred to the Trustees
- where there is no suspected illegal activity, devices may be checked using the following procedures:

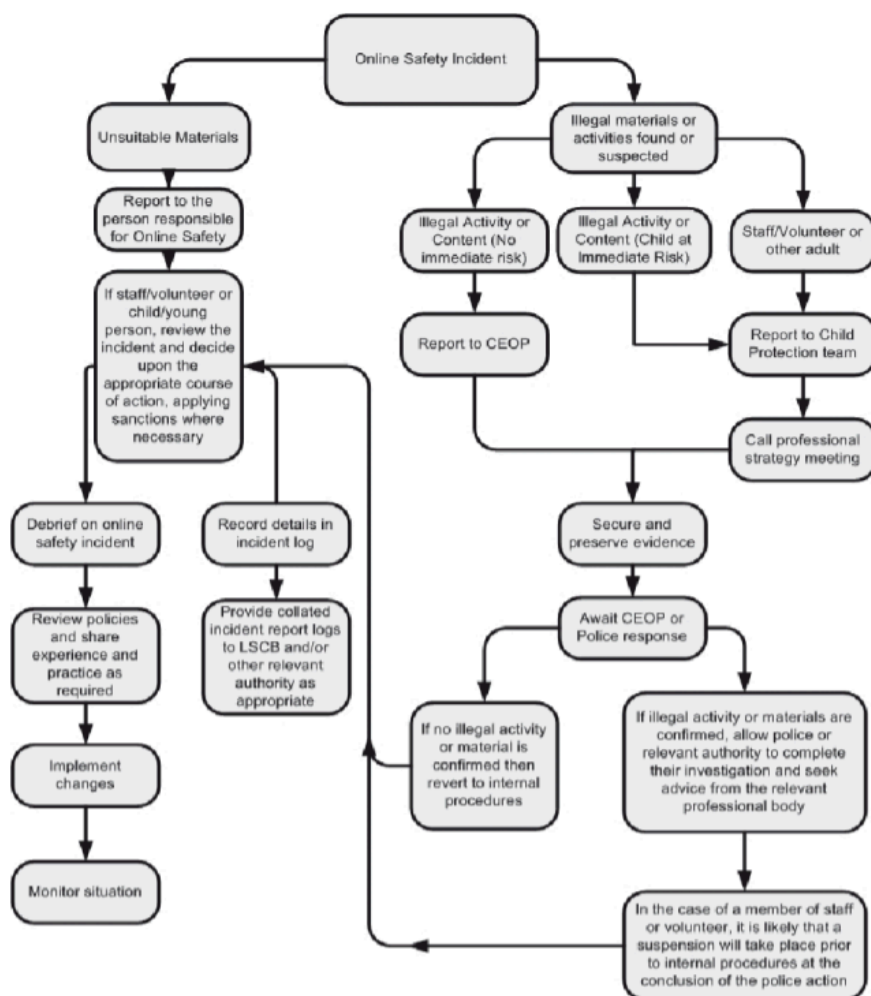
- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement of the Trustees
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
 - there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident, EAP
 - incidents should be logged
 - relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
 - those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
 - learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - trustees, through regular safeguarding updates
 - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”

will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Staff Training

Staff training will be offered during INSET days, through Educare courses and when new technologies are introduced. Advice and guidelines on using technology is given regularly when the need arises. Technical staff members have a key role in maintaining a safe infrastructure at the school and keeping abreast with the rapid succession of technical developments.

Procedure for reporting an incident online - Flowchart



Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; English etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches which should be filtered by Securly.
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit using Securly Classroom.
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can unblock the site for that lesson using Securly Classroom by pushing through the URL. If the site is still blocked, a request can be made to The Systems Manager.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Please refer also to the School's Safeguarding, Behaviour, Anti-bullying, PSHEE, and RHSE Curriculum policies, and for further information regarding incidents of cyber bullying. These will be provided by following a planned e-safety programme provided as part of Digital Learning, PSHEE and other lessons

Contribution of Learners

The School acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of technology ambassadors
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Filtering

- the School filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the School manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the [Internet Watch Foundation CAIC](#) list and the police assessed list of

terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided differentiated user-level filtering
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- If necessary, the school will seek advice from, and report issues to, the [SWGfL Report Harmful Content site](#).

Monitoring

The School has monitoring systems in place to protect the school, systems and users:

- The School monitors all network use across all its devices and services. An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.
- There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The School follows the [UK Safer Internet Centre Appropriate Monitoring guidance](#) and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring including using Securly Classroom (adult supervision in the classroom)
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to E-safety Co ordinators and Safeguarding Leads

Safeguarding, Filtering and Monitoring Outside of School Hours

During term time, our filtering and monitoring systems are actively overseen by staff. However, there are periods when the school is closed or operating at reduced capacity, such as half terms and school holidays. During these times, our approach is as follows:

Filtering (always active)

All school-managed devices and networks continue to be protected by filtering systems at all times. These systems are designed to block access to inappropriate, harmful or illegal content and remain fully operational whether pupils are in school or at home.

Monitoring (proportionate approach outside school hours)

Our monitoring systems continue to operate during evenings, weekends and holiday periods. They may identify and log any concerning online behaviour or searches.

NB Outside of normal school hours, alerts are not reviewed in real time. Instead, they are recorded and reviewed by safeguarding staff when the school reopens or when staff return to duty.

Support during closure periods

When school is not in session, immediate safeguarding support is not provided through school systems. If a pupil is using a school-managed device during these times, parents and carers play an important role in supervising and supporting their child's online activity. This includes:

- Discussing safe online behaviour
- Monitoring device use where appropriate
- Ensuring age-appropriate access to apps, games and websites

Where appropriate, parents and carers may also take a more active role in monitoring their child's device when it is used outside of school hours by joining Securly Home.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies in the cloud
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Trust Network Manager
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the Head of Digital Learning, who will keep an up-to-date record of users and their usernames
- It is recommended that staff change their password regularly, using a combination of words, numbers and special characters. Staff should avoid using predictable words.
- Chrome accounts will be deactivated or suspended when you leave school.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.

- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.

Email

It is important that staff are aware of the risks of email:

- Sending or forwarding emails with any libellous, defamatory, offensive, racist or obscene remarks
- Unlawfully forwarding confidential information, the staff member and the Radley Schools Group can be held liable
- Unlawfully forwarding or copying messages without permission, the staff member and the Radley Schools Group can be held liable for copyright infringement
- Sending an attachment that contains a virus, the staff member and the Radley Schools Group can be held liable

Personal Email

Although the Radley Schools Group's email system is meant for business use, Chandlings Prep allows limited personal usage if it is reasonable and does not interfere with work.

Best Practises

When using emails, adhere to the following guidelines:

- Write well-structured emails and use short, descriptive subjects
- Signatures must include staff name, job title, and the school logo, address and contact details
- Users must spell check all emails prior to transmission
- Do not send unnecessary attachments
- Do not click on any links or open any attachments of unsolicited or suspicious looking emails. These messages could infect your computer with a virus
- Take care when sharing and email thread - as this can be forwarded on

Staff Devices

Mobile phones are permitted on the premises, but any staff teaching EYFS should not be using them when they are in the presence of children.

Staff should limit use of their mobile phones to designated areas such as the staff room and in classrooms when the children are out at another activity. There are occasions in which staff may be required to check something on their phones, in public areas, for work purposes. Examples may include: two factor authentication. Sports staff may need to use their mobile phones to contact the school or be contacted whilst they are out at a remote sports location or facility. Tablet devices should only be used for professional reasons in school and social media should not be accessed during the school day, either via phone or tablet applications. There may be instances where social media is used for school purposes e.g. Chandlings Prep Twitter and Facebook. Recreational/ personal/ social use of mobile devices is not

deemed appropriate.

Personal mobile phones should not be used to take photographs or record videos of children. The school cameras/phones should be used instead.

Please refer to our Staff Mobile Phone policy and Safeguarding Policy for more details.

Pupil Devices

- Mobile phones, iPods and other personal electronic devices are not permitted at school on a normal working day. Exceptions are made during excursions, and the conditions of the equipment use are stated clearly beforehand by the trip coordinator. Smartwatches are **not permitted** in school under any circumstances. This includes watches with the following: Camera facilities (including sound recording). Capability to send and receive messages. Capability to independently access the internet and is therefore not part of the school's filtering and monitoring system.
- Cameras and Webcams used by children will be monitored by teachers and will be used solely for creating lesson content and not for public broadcast or communicating via any form of social media.
- Pupils will often share resources and work content in order to accomplish a task. This must be done in an environment where respect is paid to other pupil's work and content must be "looked after" so that pupils can trust their peers and collaborate in a positive manner.
- Pupils have access to monitored Chromebooks for the purpose of completing schoolwork.

Involvement with Parents

We seek to work closely with parents and guardians in promoting a culture of e-safety. We understand the need for maintaining open channels of communication between school and home with regards to pupil behaviour while using the internet. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. Head of Digital Learning and Pastoral leads will from time to time take initiatives to promote discussion and raise a level of consciousness within our school community on topical points relating to e-safety. We are happy for parents to discuss with the Head of Digital Learning and Head of Pastoral Care the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

Appendix A

Acceptable Use Agreement – staff

For my professional and personal safety:

- I understand that the school will monitor my use of the Computing systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school Computing systems (e.g. laptops, email) out of school
- I understand that the school Computing systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person
- I understand that I will not take photographs of children on any personal device

I will be professional in my communications and actions when using school Computing systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images.
- I will only communicate with pupils and parents/carers, in relation to school business, using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will not upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials

- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure school network, it must be encrypted or password protected.
- I will report any damage or faults involving equipment or software

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, suspension, or a referral to Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police

Appendix B

Acceptable Use Agreement- Children (Prep department)

This agreement will help keep me safe and help me to be fair to others.

1. I learn online – I use the school's internet and Chromebooks for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. I ask permission – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. I am creative – I don't just spend time on apps, sites and games looking at things from other people. I try not to get distracted

a friend – I won't share anything that I know another person wouldn't want to be shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.

5. I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. I am a careful clicker – I don't click on unexpected links or popups. If I am not sure I ask an adult.
7. I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about. I communicate respectfully with my peers and adults. I am careful when someone wants to be my friend.
10. I don't do live videos (livestreams) on my own – I check with a trusted adult before and I check if it is allowed.
11. I keep my body to myself online – I never show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it.
12. I tell my parents what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
13. I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends.
14. I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay part of my digital footprint forever.
15. I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
16. I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
17. I respect people's work – I only edit or delete my own digital work. If I am collaborating with someone we work together on a piece of work.
18. I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.
19. I am reliable and can be trusted - My teachers are trusted adults, therefore they can view my digital activity and monitor my use of the school technology so that they can guide me and offer help where necessary.
20. I respect my school - I am entrusted to use technology in a respectful way. If I do not use it in this way, I accept that I may be restricted from using technology by the Head.

Appendix B

Acceptable Use Agreement- Children (Pre Prep department)

This agreement will help keep me safe.

I ask permission – At home or school, I only use the devices, apps, sites and games I am allowed to, at the right times.

I learn online – I will only use activities that a teacher or adult has allowed me to use

I am careful - I will take care of the Chromebooks and other equipment

I will ask for help - from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

I will report - and tell a teacher or adult if I see something that upsets me on the screen

I am a friend – online and in person

~~~~~

All children should agree to these points before using Chromebooks

## Appendix C

### Acceptable Use Agreement- Parents/Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the KS1 and KS2 acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to acknowledge the permission form below by following the Google Form. We hope you support the school in this important aspect of the school's work.

## Appendix D

### Acceptable Use Agreement- Visitors

As a visitor to the school I recognise that it is my responsibility to follow school online safety advice and that I have a responsibility to ask if I am not sure of a procedure.

This is not an exhaustive list and all visitors are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

This acceptable use policy is intended to ensure:

that community users of school digital technologies will be responsible users and stay safe while using these systems and devices

that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

that users are protected from potential harm in their use of these systems and devices

#### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

I understand that my use of school systems and devices will be monitored

I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.

I will not try to upload, download or access any materials which are illegal (anything covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will not access, copy, remove or otherwise alter any other user's files, without permission.

I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.

I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

I will not disable or cause any damage to school equipment, or the equipment belonging to others.

I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems and my own devices within these guidelines.