St. Paul's Dorking
Church of England (Aided) Primary School

('the School')

Online Safety Policy

Policy date: Apr 24 Full review date: Apr 25 (*review yearly or as needed*)

Associated Policies	
Title	**Start Date**
Anti – Bullying	2023
Behaviour	Oct 23
Child Protection and Safeguarding	Sep 23
Computing	Mar 24
Data Protection / GDPR	Oct 22
PSHE	Mar 21
Use of AI	(merged)
Use of Mobile Technology *(as defined at 1.1.3)*	(merged)
Use of Images	(merged)
Social Media	(merged)
Online Platform ('**Teams**')	(merged)

Appendices	
1	Acceptable Use Policy EYFS/KS1 (Agreement and Display)
2	Acceptable Use Policy KS2 (Agreement and Display)
3	Staff, Governor, Contractor, Volunteer and Visitor Acceptable Use Agreement/Code of Conduct (including trips)
4	Parent/Carer Consent Form: Use of Images and Online Safety
5	Staff Device/Laptop Loan Agreement
6	Pupil Device/Laptop Loan Agreement
7	Staff OLS Training Needs Audit

Member of Staff with Responsibility – Alexandra McLeod ('**OLS Lead**')

St. Paul's Dorking
Church of England (Aided) Primary School

Contents

St. Paul's Dorking
Church of England (Aided) Primary School

('the School')

ONLINE SAFETY POLICY

Policy date: Mar 2024 Full review date: Mar 2025 (review yearly or as needed)

1. Aims

1.1. Our School aims to:

1.1.1. Have robust processes in place to ensure the online safety of pupils, staff, visitors, contractors, volunteers and governors;

1.1.2. Identify and support groups of pupils that are potentially at greater risk of harm online than others;

1.1.3. 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** and including **wearable technology**, (which we will refer to under the umbrella term of '**Mobile Technology**'); and

1.1.4. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1.2. Keeping Children Safe in Education (KCSIE) (September 2023) classifies online safety risks into four key categories of risk: **content, contact, conduct and commerce**. These are known as the **4Cs of online safety**. Our approach to online safety is based on addressing these 4 categories of risk which are defined as:

1.2.1. **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

1.2.2. **contact**: being subjected to harmful online interaction with other users; for example: 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.

1.2.3. **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, 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.

1.2.4. **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. Legislation and guidance

2.1. This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Schools on:

2.1.1. Teaching online safety in Schools

2.1.2. Preventing and tackling bullying and cyber-bullying: advice for Headteachers and School staff

2.1.3. Searching, screening and confiscation

2.1.4. It also refers to the DfE's guidance on protecting children from radicalisation.

2.1.5. 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.

2.1.6. The policy also considers the National Curriculum computing programmes of study.

3. Links and Reviewing

3.1. The Online Safety Policy is an integral part of the School's safeguarding responsibilities and relates to other policies including those for Behaviour, Computing, Online Platforms, Safeguarding, Mobile Technology, Acceptable Use, Anti-Bullying, PSHE, Data Handling, Social Media, Use of AI and the Use of Images.

3.2. The School has an Online Safety Committee who meet twice a year. The committee is made up of the OLS Lead, OLS Portfolio Governor, the Designated Safeguarding Lead ('**DSL**') and the IT Technician/Deputy Designated Safeguarding Lead ('**IT/DDSL**').

3.3. This Online Safety Policy has been written by the School, building on best practice and Government guidance. It has been agreed by the Online Safety Committee and approved by Governors.

3.4. The Online Safety Policy and its implementation will be reviewed annually or as necessary in response to events or updated best practice.

3.5. The Online Safety Policy covers the use of all technology which can access the School Network and the internet or which facilitates electronic communication from School to beyond the bounds of the School site. This includes, but is not limited to, workstations, laptops, Mobile Technology, tablets, remote access servers and hand-held games consoles used on the School site and any cloud operating systems, including the O365 Suite and Microsoft Teams Online Platform ('**Teams**'), and Network storage; all of which are part of the School technology provision ('**the School Network**').

3.6. The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff, a pupil or visitor.

4. Roles and Responsibilities

4.1. The **OLS Lead** will:

4.1.1. ensure that staff (including contractors and agency staff) understand this policy and that it is being implemented consistently throughout the School;

4.1.2. review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;

4.1.3. Take the lead, with support from the IT/DDSL and the DSL, on understanding the filtering and monitoring systems and processes in place on School devices and School networks;

4.1.4. Work with the IT Infrastructure Manager ('**ITIM**') to make sure the appropriate systems and processes are in place;

4.1.5. Regularly, and at least every fortnight, work with the IT/DDSL to test, challenge and log all Mobile Technology access to the internet via the School Network to ensure the effectiveness of the filtering and monitoring systems and processes and report any breaches, or potential breaches, to the School's IT Service Provider, Eduthing Ltd ('**Eduthing**') to rectify;

4.1.6. Work with the DSL, ITIM, IT/DDSL and other staff, as necessary, to address any online safety issues or incidents;

4.1.7. Review all online safety issues and incidents to ensure this policy and all relevant procedures are reviewed and updated as needed;

4.1.8. Update and deliver, or arrange delivery of, staff training on online safety (see Appendix 4 for a self-audit for staff on online safety training needs which will be regularly undertaken and training adjusted accordingly);

4.1.9. Liaise with other agencies and/or external services if necessary;

4.1.10. Provide twice yearly audits of online safety in School to the Governing Board via the Online Safety Committee;

4.1.11. Provide regular online safety updates, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

4.1.12. This list is not intended to be exhaustive.

4.2. The **Designated Safeguarding Lead** ('**DSL**'). Details of the School's DSL (and DDSLs) are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions. The DSL takes overall responsibility for online safety in School and will meet termly with the OLS Lead to ensure the responsibilities above have been carried out. The DSL is responsible for:

4.2.1. Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the School;

4.2.2. Working with the OLS Lead, Headteacher and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;

4.2.3. In conjunction with the OLS Lead, understand the filtering and monitoring systems and processes in place on School devices, Mobile Technology and School networks;

4.2.4. Working with the OLS Lead and ITIM to make sure the appropriate systems and processes are in place;

4.2.5. Working with the Headteacher, OLS Lead, ITIM and other staff, as necessary, to address any online safety issues or incidents;

4.2.6. Managing all online safety issues and incidents in line with the School's Child Protection Policy;

4.2.7. Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;

4.2.8. Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School behaviour policy;

4.2.9. This list is not intended to be exhaustive.

4.3. The **ITIM** and/or the **Eduthing** is responsible for:

4.3.1. Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on School devices, Mobile Technology and School networks, which are reviewed in conjunction with the ITIM and updated at least termly 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;

4.3.2. Ensuring that the School's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;

4.3.3. Conducting a full security check and monitoring the School's IT systems on a regular basis and in response to notified or identified incidents;

4.3.4. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files as required and/or as notified by the OLSLead and IT/DDSL as a result of filtering and monitoring system checks;

4.3.5. This list is not intended to be exhaustive.

4.4. The **Governing Board** has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

4.4.1. The Governing Board will facilitate meetings twice a year with the OLS Committee to discuss online safety and review the prepared OLS Audit.

4.4.2. All governors will:

- Ensure they have read and understand this policy;
- Agree and adhere to the terms of acceptable use of the School's IT systems and School's Network and the internet (appendix 3);
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-School approach to safeguarding and related policies and/or procedures;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

4.5. **The Headteacher** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the School.

4.6. All **staff** and **volunteers,** including contractors and agency staff, volunteers and visitors are responsible for:

4.6.1. Maintaining an understanding of this policy;

4.6.2. Implementing this policy consistently;

4.6.3. Agreeing and adhering to the terms on acceptable use of the School Network and the internet, reading and signing the AUP (on joining and as revised) and ensuring that pupils follow the School's terms on acceptable use (appendices 1 and 2);

4.6.4. Knowing that the OLS Lead and DSL are responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting it to the OLS Lead or DSL immediately via CPOMS;

4.6.5. Following the correct procedures (in writing via email) by requesting access to the OLS Lead or DSL if they need to bypass the filtering and monitoring systems for educational purposes;

4.6.6. Working with the OLS Lead and DSL to ensure that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy;

4.6.7. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour Policy;

4.6.8. Responding appropriately and in a timely manner to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here';

4.6.9. This list is not intended to be exhaustive.

4.7. **Parents/carers** are expected to:

4.7.1. Notify the Headteacher, the OLS Lead or a member of Staff of any concerns or queries regarding this policy;

4.7.2. Ensure their child has read, understood and agreed to the terms on acceptable use of the School Network and internet (appendices 1 and 2);

4.7.3. Complete a Parent/Carer Consent Form at the start of EYFS and KS2 (or when material amendments are made and notified to them);

4.7.4. Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

4.8. **Visitors** and members of the community

4.8.1. Visitors and members of the community who use the School Network (including, but not limited to, allowed internet access on any supplied channels) will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on Acceptable Use (appendix 3).

5. Educating pupils about online safety

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

5.2. In **Key Stage (KS) 1**, pupils will be taught to:

5.2.1. Use technology safely and respectfully, keeping personal information private;

5.2.2. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

5.3. Pupils in **Key Stage (KS) 2** will be taught to:

5.3.1. Use technology safely, respectfully and responsibly;

5.3.2. Recognise acceptable and unacceptable behaviour;

5.3.3. Identify a range of ways to report concerns about content and contact.

5.4. By the **end of primary school**, pupils will know:

5.4.1. That people sometimes behave differently online, including by pretending to be someone they are not;

5.4.2. 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;

5.4.3. The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;

5.4.4. How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;

5.4.5. How information and data is shared and used online;

5.4.6. What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);

5.4.7. How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know;

5.4.8. The safe use of social media and the internet will also be covered in other subjects where relevant;

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

5.4.10. Why Internet and digital communications are important.

5.5. All communication between staff and pupils or families will take place using School equipment and/or School email accounts (including via Teams).

5.6. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

5.7. The School Internet access is provided by Talk Straight (Schools Broadband), and includes appropriate filtering for staff and pupil users provided by NetSweeper and managed and monitored by Eduthing, the OLS Lead and IT/DDSL.

5.8. The School uses materials from Project Evolve, NSPCC, Thinkuknow and UK Safer Internet Centre, to educate pupils in the safe use of social networking and the wider internet. The scheme is delivered half-termly and in longer units and focus days when appropriate.

5.9. The School will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

5.10. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5.11. Where possible, pupils are encouraged to verify the information they find online with cross-referenced trusted sites and other sources, e.g. books.

5.12. Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon, Hector Protector and by telling a trusted adult.

6. Educating parents/carers about online safety

6.1. The school will endeavour to raise parents/carers' awareness of internet safety via the OLS pages on our website, via Teams, in Newsletters or any other communications home. This policy will also be available to parents/carers.

6.2. Online safety will also be covered during parents' evenings via a presentation in the Hall.

6.3. The school will let parents/carers know:

6.3.1. What systems the school uses to filter and monitor online use;

6.3.2. 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. This will be generally available via the Year Group Curriculum Overviews on the Website.

6.3.3. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

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

7. Cyber-bullying (**see Anti-Bullying Policy for details**)

7.1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (For further information please see the Anti-Bullying Policy and School Behaviour Policy.).

8. Artificial intelligence ('AI')

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

8.2. The School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

8.3. The School will treat any use of AI to bully pupils in line with our Anti-Bullying and/or Behaviour policies.

8.4. Staff should be aware of the risks of using AI tools whilst they are still being developed and the ITIM will carry out a risk assessment where new AI tools are being used universally by the School.

8.5. The School has a commitment to use AI fairly and safely.

8.6. Appropriate use of AI

Staff and pupils will be supported to understand that AI can be positively used as a tool to support teaching and learning, but can also be used by them and others in a negative way.

8.6.1. Staff and pupils should use AI positively to:

- use as smart search engines that present information in ways that are easy to read and understand;
- generate ideas, topics and writing prompts;
- use within their own work, but always attribute AI text and images properly.

8.6.2. Staff and pupils should not use AI:

- to avoid doing their own work;
- to copy text or images from AI programs without proper attribution;
- text or images without fact-checking and exploring potential plagiarism issues;
- when it is expressly forbidden (i.e. within an assignment).

8.7. Responsible use of AI

8.7.1. Personal data should not be shared with AI bots without first confirming the validity of the App or site.

8.7.2. AI should never be used to invade the privacy of others.

8.8. Reporting AI Misuse

Staff and/or pupils should report AI misuse to the OLS Lead, DSL or a trusted adult in the same way that they would for any other OLS concern.

9. Managing Access and Security of the School Network

9.1. The School will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between the managed School Network and the more open systems outside School.

9.2. School Network security

9.2.1. The School will use a recognised internet service provider or regional broadband consortium. At present the School is using Talk Straight (Schools Broadband).

9.2.2. The School will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable. Netsweeper and SENSO are currently being used for filtering purposes.

9.2.3. Access to School networks (including Teams) will be controlled by age appropriate passwords for children and strong personal passwords for adults.

9.2.4. Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy. SENSO is currently being used for this purpose.

9.2.5. The security of the School Network is monitored and reviewed regularly by Eduthing.

9.2.6. The School will ensure, via Eduthing, that its networks have virus and anti-spam protection.

9.2.7. Filtering and monitoring systems are managed and checked by the ITIM, ITTech/DDSL and DSL and will be supervised by the OLS Committee and have clear procedures for reporting issues.

9.2.8. The School will ensure that access to the internet via School equipment for anyone not employed by the School is filtered and monitored.

9.2.9. Security strategies will be discussed with Eduthing, Schools Broadband and Surrey CC as necessary and reviewed termly.

10. Acceptable use of the School Network

10.1. All pupils, parents/carers, staff, governors, contractors and volunteers are expected to sign an agreement regarding the acceptable use of the School Network (appendices 1, 2, 3 and 4). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

10.2. Use of the School Network must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

10.3. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

10.4. More information is set out in the Acceptable Use Agreements at appendices 1, 2 and 3.

11. Use of Mobile Technology in School

11.1. Pupil Use of Mobile Technology in School

11.1.1. For pupils who are walking to or from School alone (KS2), pupils may bring a **mobile phone** into school, but a permission slip must be signed and handed in to the Office before the mobile phone is brought to School. The mobile phone must be handed in to the Class Teacher (or Supply), as soon as the pupil arrives at School, to be locked away and will only be returned when the pupil leaves School for the day. The mobile phone should be labelled with the pupil's initials and be turned off before being handed in.

11.1.2. Any mobile phone not handed in as the pupil arrives, or any other Mobile Technology which is brought to School, will be confiscated and placed in the School office for safekeeping. Any confiscated Mobile Technology will need to be collected from the School office by Parents/Carers at their earliest convenience.

11.1.3. If a pupil needs to contact a parent/carer during the School day, this must be done via the School office.

11.1.4. If the pupil is attending an after-school club, the mobile phone will be given to the adult running the club for safekeeping until the end of the club. This includes before or after school provision such as Breakfast Club or Action House.

11.1.5. Other Mobile Technology (as defined in 1.1.3 above) must not be brought to School. This includes, but is not limited to, all wearable technology such as smart watches or fitness trackers.

11.2. Staff Use of Mobile Technology in School

11.2.1. Staff (including governors, volunteers, contractors, visitors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present. Use of personal mobile phones, and other Mobile Technology for functions which access the internet (i.e. picking up messages or emails on a Smart Watch) or capture images, must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

11.2.2. There may be circumstances in which it is appropriate for a member of staff to have use of Mobile Technology during contact time. For instance:

- For **emergency** contact by their child, or their child's school;
- In the case of acutely ill dependents or family members;

The Headteacher will decide on a case-by-basis whether to allow for temporary special arrangements and written permission must be sought and given and any use of such Mobile Technology must be limited and away from pupils.

11.2.3. If special arrangements are not deemed necessary, school staff can use the school office number (01306 883547) as a point of emergency contact.

11.2.4. Data protection - Staff must not use their personal mobile technology to process school related personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Bard). For further guidance, please refer to the Data Protection Policy.

11.2.5. Safeguarding

- Staff must not give their personal contact details to parents/carers or pupils, including connecting through social media and messaging apps.
- Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.
- Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it is necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.
- Staff may use personal photographic equipment at their own risk, but it must be fitted with an exclusive use SD card provided by, and retained by, the School.
- Staff may need to use their personal Mobile Technology for Two Factor Authentication ('**TFA**') purposes such as CPOMS, but this must be done when pupils are not present.

11.2.6. Staff may connect their Mobile Technology to the School Internet via the BYOD channel using their normal Network login details to access the channel.

11.2.7. Using personal Mobile Technology for work purposes. In some circumstances, it may be appropriate for staff to use personal Mobile Technology for work. Such circumstances may include, but are not limited to:

- Emergency evacuations.
- Emergency situations during off-site or residential trips.

For off-site or residential trips, staff should take a School mobile phone (when available).

11.2.8. If staff are required to use their personal Mobile Technology for emergency or off-site/residential trips, they must:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct;
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil;
- Refrain from using their phones to contact parents/carers except by using their Network's block number code. If possible, contact should be made via the School office.

11.2.9. Work phones may be issued to adults who are leading an off-site or residential trip or in an emergency. Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

In these situations, staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct.

11.2.10. Sanctions - Staff that fail to adhere to this policy may face disciplinary action. See the school's staff disciplinary policy/code of conduct for more information.

11.3. Parents/carers, volunteers and visitors use of Mobile Technology in the School

11.3.1. Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it is a public event (such as a school fair), this includes taking pictures or recordings of their own child;
- Using any photographs or recordings taken at a public event for personal use only, and not posting on social media without first obtaining specific consent from all parents/carers of the children in the photographs/recordings.
- Not using Mobile Technology when working with pupils or when pupils are present.

11.3.2. Parents/carers, visitors and volunteers will be informed of the rules for Mobile Technology use when they sign in at the School office.

11.4. Parents/carers, volunteers and visitors use of Mobile Technology on School related trips or at School related events

11.4.1. Parents/carers or volunteers present at school trips, residential visits, clubs or events **must not**:

- Use their personal Mobile Technology when children are present;
- Use their personal Mobile Technology to take photos or recordings of pupils, their work, or anything else which could identify a pupil;

11.5. Parents/carers must use the School office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal Mobile Technology during the school day.

11.6. All parents/carers, volunteers and visitors will be asked to sign a summary Acceptable Use Agreement ('**AUA**') confirming their understanding of the relevant sections of this Policy.

11.7. Loss, theft or damage

11.7.1. Pupils who have permission to bring their mobile phones to school must ensure that phones are labelled with their initials and are immediately handed in to their Class Teacher (or Supply) on arrival.

11.7.2. It is suggested that all pupils secure their mobile phones with a password or pin code to protect against unauthorised access.

11.7.3. Staff must also secure their personal Mobile Technology, as well as any work phone provided to them. Failure by staff to do so could result in data breaches.

11.7.4. The school accepts no responsibility for Mobile Technology that is lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

11.7.5. Any confiscated Mobile Technology will be stored in the School office and will be available for collection by a parent/carer at their earliest convenience.

12. Staff using work devices outside school

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

12.1.1. Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);

12.1.2. Making sure the device locks if left inactive for a period of time;

12.1.3. Not sharing the device among family or friends;

12.1.4. Liaising with Eduthing to install anti-virus and anti-spyware software;

12.1.5. Liaising with Eduthing to keep operating systems up to date by always installing the latest updates;

12.1.6. Not storing any data or School information locally on the device, but instead using either remote access to work directly on the School Network or storing to OneDrive cloud storage provided with their School O365 account.

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

12.3. Work devices must be used solely for work activities.

12.4. If staff have any concerns over the security of their device, they must seek advice from the ITIM or Eduthing immediately.

13. E-mail

13.1. Pupils are not issued with School e-mail accounts. However, the use of email is discussed in Online Safety lessons and pupils are taught how to manage email.

13.2. Pupils are taught how to deal with offensive e-mail and how to report to a parent/carer or trusted adult.

13.3. Pupils are taught that they must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

13.4. The School uses year-group based email accounts and these will be monitored and operated by the year group teaching team.

13.5. Staff to parent communication must only take place via a School email address or from within Teams and will be monitored. It is recommended that staff use their year group email account to contact parents/carers or ask the School office to forward emails to parents/carers.

13.6. Staff must not email directly to a pupil personal email account and should only use email addresses as notified by parents.

13.7. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. All suspect emails must be immediately forwarded to Eduthing (itsupport@eduthing.co.uk) to be investigated.

13.8. The forwarding of chain letters or their current equivalents (e.g. 'memes' or viral content) is not permitted.

14. The School web site and other published content

14.1. The contact details on the School's website, X, Facebook or other social networking platforms or on Teams, should be the School address, web address, e-mail and telephone number.

14.2. Staff or pupils' Personal Information (such as data, including photographs, held on SIMS or in other areas on the School Network ('**Personal Information**')) will not be published, other than the names, official photographs and responsibilities of staff.

14.3. The Website Officer, Office Manager and ITIM have responsibility for maintaining and reviewing the website. The Website Officer has overall responsibility to ensure that content is accurate and appropriate.

15. Use of pupils' images

15.1. Written permission from parents or carers is obtained via a consent form on joining the School and revised at the start of KS2 (Year 3) which may allow photographs of pupils to be published on the School website, in School newsletters or sports or activities reports or in other publicity, unless objected to.

15.2. If consent to publish images is withdrawn, no further images will be shared or published but it may not be possible to delete images that have already been shared or published.

15.3. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified e.g. via name tag or a book label. The School will look to seek to use group photographs rather than full-face photos of individual children where photos are published to social media.

15.4. Pupils' full names will not be used on the School web site, particularly in association with photographs.

15.5. Parents are clearly informed of the School policy on image taking and publishing.

15.6. Images will be stored securely on the School Network in accordance with our safeguarding policy and data protection laws. Images and recordings will be deleted within two years of the pupil leaving the School.

15.7. The School does not permit staff or volunteers to use any personal Mobile Technology to take images or recordings of children. Only cameras, devices or cameras containing SD cards belonging to the School or devices used exclusively for School use and linked to a School account will be used.

15.8. The School will reduce the risk of images being copied and used inappropriately by:

15.8.1. only using images of children in appropriate clothing (including safety wear if necessary);

15.8.2. avoiding full face and body shots of children taking part in activities such as swimming where there may be a heightened risk of images being misused;

15.8.3. using images that positively reflect young people's involvement in an activity;

15.9. Parents must only use images or recordings taken at public School events (i.e. Sports Day) for personal use, and must not post images or recordings on social media without first obtaining specific consent from all parents/carers of the children in the images or recordings.

15.10. The School will announce the requirement at 15.9 at the start of all public School events.

15.11. Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different Schools, countries and cultures.

15.11.1. A webcam will only be used in appropriate circumstances such as a normal class setting.

15.11.2. Both children and staff will be made aware of when a webcam is in use.

15.12. The School uses CCTV in some areas of School property as a security measure. CCTV cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

15.13. Staff will supervise and maintain control over any photographing pupils do during in-School or off-site activities.

15.14. Children may use a class set of cameras for certain IT work and during photography/newspaper clubs. Photos taken on these cameras will only be stored on School computers and used appropriately as per the Online Safety policy.

15.15. The School has procedures in place for reporting the abuse or misuse of images of children as part of our child protection procedures. We will ensure that all staff know the procedures to follow to keep children safe.

16. Social Media

16.1. Social media (e.g. Facebook, X, WhatsApp) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or Roblox and video sharing platforms such as You Tube have social medial elements to them.

16.2. The use of external social networking sites in School is not allowed by pupils, other than for supervised use in respect of the pupils' X reporting account, or to demonstrate safe use in lessons.

16.3. Within School, a limited range of social networking services may be provided via Teams. Their introduction is staggered by age, allowing staff to introduce children to social networking in a safe and monitored environment.

16.4. Pupils and parents will be advised that the use of social network spaces outside School brings a range of dangers for primary aged pupils through parent Online Safety information and materials available via the website.

16.5. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

16.6. Use of video services such as Teams, Skype, Google Hangouts and Facetime will be monitored by staff if used during a lesson. Pupils must ask permission from a member of staff before making or answering a video call.

16.7. Staff and pupils should ensure that their online activity, both in School and out considers the feelings of others and is appropriate for their situation as a member of the School community.

17. Online Platform ('Teams')

17.1. The use of Teams is subject to the expectations and requirements of this Online Safety Policy and staff and pupils must ensure that all communications through Teams are appropriate and respectful.

17.2. Teams will primarily be used to assign homework and special projects. However, it will also be used to deliver online learning in the event of a closure of the School.

17.3. Pupils are reminded that the chat function within Teams is to allow them and their teachers to communicate about the work set or questions they may have. Any misuse of this function may necessitate withdrawing the chat function either temporarily or permanently from a pupil.

17.4. Any misuse of the chat function should immediately be reported to the class teacher or the School office.

17.5. The School subscribes to a number of associate online platforms such as TTRockstars or MyMaths.com. These are closely monitored by the class teacher and all data is encrypted and protected via the School's management information system.

18. Managing emerging technologies

18.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

18.2. Pupil Mobile Technology is not allowed in School and will not be used during lessons or formal School time.

18.3. As the use of iPads and other tablet devices becomes more widespread in schools, they will be protected by a code lock where appropriate (for individual use) or kept in a locked cabinet and will be used appropriately to enhance lessons and teachers' work.

18.4. Games machines including Playstation, Xbox and Wii have Internet access which may not include filtering. Children are educated about their safe use through Online Safety lessons and PSHE.

19. Protecting Personal Information

19.1. The School has a separate Data Handling Policy. It covers the use of biometrics in School, access to pupil and staff Personal Information on and off site and remote access to the School Network.

20. Policy Monitoring and review

20.1. The school is committed to ensuring that this policy has a positive impact of pupils' education, behaviour and welfare. When reviewing the policy, the school will consider:

20.1.1. Feedback from parents/carers and pupils

20.1.2. Feedback from teachers

20.1.3. Records of behaviour and safeguarding incidents

20.1.4. Relevant advice from the Department for Education, the local authority or other relevant organisations

21. Policy Decisions

21.1. Authorising Internet access

21.1.1. All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, supply teachers, work experience trainees, IT technicians and governors) must read and sign an 'Acceptable Use Agreement ('**AUA**') (appendix 3) before using any part of the School Network.

21.1.2. The School will maintain a current record of all staff and pupils who are granted access to the School Network.

21.1.3. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

21.1.4. At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.

21.1.5. Parents will be asked to sign and return a consent form for all children in every Key Stage (appendix 4) to allow use of technology by their pupil.

21.1.6. Any person not directly employed by the School will be asked to sign an AUA before being given access to the internet via the School Network.

21.2. Assessing risks

21.2.1. The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will not appear on a School computer. Neither the School nor SCC can accept liability for the material accessed, or any consequences of Internet access.

21.2.2. The School audits IT use and emergence of new technologies to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

21.3. Handling Online Safety complaints

21.3.1. Complaints of misuse of the School Network will be dealt with by the OLS Lead, DSL or a senior member of staff and in accordance with the School behaviour policy.

21.3.2. Any complaint about staff misuse must be referred to the Headteacher.

21.3.3. Complaints of a child protection nature must be dealt with in accordance with School child protection procedures.

21.3.4. Pupils and parents will be informed of the complaints procedure.

21.3.5. Pupils and parents will be informed of consequences for pupils misusing the School Network.

21.3.6. Complaints may be passed onto the LEA and the police if this is felt to be appropriate.

21.4. Community use of the Internet

21.4.1. Members of the community and other organisations using the School internet connection will have signed an AUA (appendix 3) so it is expected that their use will be in accordance with the School Online Safety Policy.

22. Training

22.1. 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.

22.2. 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, focus days (i.e. SID) and staff meetings).

22.3. By way of this training, all staff will be made aware that:

22.3.1. Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

22.3.2. Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

22.3.3. 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

22.4. The DSL and DDSLs will undertake child protection and safeguarding training, which will include OLS, at least every 2 years. They will also update their knowledge and skills on the subject of OLS at regular intervals, and at least annually.

22.5. The OLS Lead will attend termly OLS Network Meetings.

22.6. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

22.7. Volunteers will receive appropriate training and updates, if applicable.

22.8. More information about safeguarding training is set out in our child protection and safeguarding policy.

23. Communication of the Policy

23.1. To pupils

23.1.1. Appropriate elements of the Online Safety policy are shared with pupils as part of the OLS Curriculum.

23.1.2. Online Safety rules are posted in all School learning areas where the internet is accessed.

23.1.3. Pupils are informed that School Network and Internet use will be monitored.

23.1.4. The School uses Project Evolve scheme of work and materials from NSPCC, Thinkuknow and UK Safer Internet Centre in order to teach children about relevant Online Safety issues and instil a set of safe behaviours when accessing the internet.

23.1.5. Online Safety lessons are taught regularly throughout the School and links to the PSHE policy.

23.1.6. Pupils need to agree to comply with the pupil AUA in order to gain access to the School Network and to the internet.

23.1.7. Pupils will be reminded about the contents of the AUA as part of their online safety education.

23.2. To Staff

23.2.1. All staff will be given the School Online Safety Policy and its importance explained.

23.2.2. All staff must sign and agree to comply with the staff AUA in order to gain access to the School Network and to the internet.

23.2.3. All staff will receive Online Safety and Cyber Security training on an annual basis.

23.2.4. Staff should be aware that use of the School Network and internet is monitored and can be traced.

23.2.5. Discretion and professional conduct is essential.

23.3. To Parents

23.3.1. The School will ask all new parents to sign the parent /pupil AUA (appendices 1 or 2) and Images and OLS Agreement (appendix 4) when they register their child with the School and again when their child starts KS2.

23.3.2. Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the School brochure, on the School web site and on Teams.

23.3.3. Parents and carers will from time to time be provided with additional information on Online Safety via the website, newsletters, parent mail or leaflet in order to reinforce messages of Online Safety outside of School.

24. Staff Laptop and Computer Loans Agreement.

24.1. Any member of staff who borrows or uses a School laptop, computer or any other IT equipment must adhere to all aspects of this Online Safety Policy. This must be the case wherever the laptop, computer or other such device is being used as it remains the property of St Paul's CofE (Aided) Primary School at all times. Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the School's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense (including but not limited to, being left unattended in a vehicle or on public transport). Staff must sign the **Staff Laptop and Computer Loans Agreement** before taking the equipment away from the School premises.

25. Pupil Laptop and Computer Loans Agreement.

25.1. Pupils who meet certain criteria may apply to borrow a School laptop, or other device, for the purpose of completing School related work at home. Use of this equipment must adhere to all aspects of this Online Safety Policy. Parents/Carers and Pupils must undertake to take proper care of the equipment whilst in their possession and must sign and agree to abide by the requirements of the Pupil Laptop/Computer Loan Agreement (appendix 6). School loan equipment is limited and may not always be available for loan. Please apply via the School office (info@stpauls-dorking.surrey.sch.uk).

AMc/Apr 24

Appendix 1: EYFS and KS1 Acceptable Use Agreement ('AUA') (pupils and parents/carers)

EYFS/KS1

St. Paul's Dorking
Church of England (Aided) Primary School

ACCEPTABLE USE OF THE SCHOOL NETWORK (INCLUDING INTERNET): AGREEMENT FOR PUPILS AND PARENTS/ CARERS EYFS/KS1	
Name of pupil:	

When I use the School Network (computers and tablets etc.) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the School Network equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the School Network in my Documents folder
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the School Network, including the internet, when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the School Network and internet, and will make sure my child understands these. I have read and understood the guidance set out in the Online Safety Policy.	
Signed (parent/carer):	**Date:**

Acceptable use of the School Network and internet

Think then Click

These Online Safety Rules help us to stay safe on the Internet in Reception, Year 1 and Year 2.

Ask an adult before using the School computer equipment.

Look after the School Network equipment and tell a teacher straight away if something is broken or not working properly

We only use the internet when an adult is with us or has given us permission.

Use school computers for school work only

Be kind to others and not upset or be rude to them

Only access websites that an adult has told us to access.

Tell our teacher immediately if:

- We select a website by mistake
- We receive messages from people we don't know
- We find anything that may upset or harm us or our friends

Only use the username and password I have been given

Try my hardest to remember my username and password

Never share my password with anyone, including my friends

Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

Save my work on the School Network in my Documents folder

Check with my teacher before I print anything

Log off or shut down the computer or tablet when I have finished using it

Appendix 2: KS2 Acceptable Use Agreement ('AUA') (pupils and parents/carers)

KS2

St. Paul's Dorking
Church of England (Aided) Primary School

ACCEPTABLE USE OF THE SCHOOL NETWORK AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS KS2

Name of pupil:

I will:

- always use the School Network and the internet responsibly and for educational purposes only;
- only use the School Network and the internet when a teacher is present;
- keep usernames and passwords safe and not share these with others;
- only login to the School Network using my personal username and password.
- only edit or delete my own files.
- always ask permission before using the Internet.
- be aware that some websites and social networks have age restrictions which mean that I do not go on them.
- only visit internet sites that are appropriate for my age.
- not use Internet chat rooms.
- keep private information safe at all times and not give my, or others, name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- never send a photograph or video, or give out any other Personal Information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- tell a teacher (or trusted adult) immediately if I find any material that might upset, distress or harm me or others;
- always log off or shut down a computer or tablet when I have finished working on it;

I will not:

- access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- open any attachments in emails, or follow any links in emails, without first checking with a teacher;
- use any inappropriate language when communicating online, including in emails;
- create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- log in to the School Network using someone else's details;
- arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision;

If I bring a personal mobile phone or other Mobile Technology into school:

- I will hand in my personal mobile phone to my class teacher (or supply teacher) as soon as I arrive at School. I will ensure my parent/carer has completed a permission slip and that the device has my initials on it and is switched off before handing it in;
- I will not bring any other Mobile Technology (i.e. smart watches, fitness trackers, tablets etc.) to School and understand that, if I do, they will be confiscated and kept in the School office for safekeeping until my parent/carer is able to collect them.

I understand that the school will monitor my School Network activity and the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the School Network and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the School Network and internet, and for bringing personal electronic devices to school, and will make sure my child understands these. I have read and understood the guidance set out in the Online Safety Policy.

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

Acceptable use of the School Network and internet

Think then Click

Online Safety Rules for Key Stage 2

These rules will help to keep everyone safe and help us to be fair to others.

I will:

- Always use the School Network and the internet responsibly and for educational purposes only;
- Only use the School Network and the internet when a teacher is present;
- Keep usernames and passwords safe and not share these with others;
- Only login to the School Network using my personal username and password.
- Only edit or delete my own files.
- Always ask permission before using the Internet.
- Be aware that some websites and social networks have age restrictions which mean that I do not go on them.
- Only visit internet sites that are appropriate for my age.
- Not use Internet chat rooms.
- Keep private information safe at all times and not give my, or others, name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- Never send a photograph or video, or give out any other Personal Information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- Tell a teacher (or trusted adult) immediately if I find any material that might upset, distress or harm me or others;
- Always log off or shut down a computer or tablet when I have finished working on it;

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher;
- Use any inappropriate language when communicating online, including in emails;
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- Log in to the School Network using someone else's details;
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision;

If I bring a personal mobile phone or other Mobile Technology into school:

- I will hand in my personal mobile phone to my class teacher (or supply teacher) as soon as I arrive at School. I will ensure my parent/carer has completed a permission slip and that the device has my initials on it and is switched off before handing it in;
- I will not bring any other Mobile Technology (i.e. smart watches, fitness trackers, tablets etc.) to School and understand that, if I do, they will be confiscated and kept in the School office for safekeeping until my parent/carer is able to collect them.

I understand that the school will monitor my School Network activity and the websites I visit and that there will be consequences if I do not follow the rules.

Appendix 3: Acceptable Use Agreement ('AUA') (Staff, Governors, Contractors, Volunteers and Visitors)

STAFF, GOVERNORS, CONTRACTORS, VOLUNTEERS AND VISITORS

St. Paul's Dorking
Church of England (Aided) Primary School

ACCEPTABLE USE OF THE SCHOOL NETWORK AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, CONTRACTORS, VOLUNTEERS AND VISITORS.

The School Network and all related technologies such as email, the internet and all personal (or School issued) **Mobile Technology** (as defined in 1.1.3) are an expected part of our daily working life in School. This policy is designed to ensure that all Staff, Governors, Contractors, Volunteers and Visitors are aware of their professional responsibilities when using these technologies. All Staff, Governors, Contractors, Volunteers and Visitors who are given access to the School Network or internet or who are on the School site, are expected to sign this AUA to confirm that they are aware of the Online Safety Policy and agree to adhere at all times to its contents, the relevant points of which are summarised below.

When using the School Network and accessing the **internet** in school (or outside school on a work device if applicable),

I will not:

- use them in any way that could harm the School's or my professional reputation;
- access, or attempt to access, browse, download, upload or distribute any inappropriate material, including, but not limited to, material of a violent, criminal or pornographic nature or that could be considered offensive, illegal or discriminatory (or create, share, link to or send such material);
- access social networking sites or chat rooms;
- use improper language when communicating online, including in emails or other messaging services;
- install any software, or connect hardware or devices to the School Network without permission from the IT Infrastructure Manager.
- share my password with others or log in to the School Network using someone else's details;
- take photographs of pupils without express permission;
- use the School Network to share confidential information about the School, its pupils or staff, or other members of the community;
- access, modify or share data I am not authorised to access, modify or share;
- promote private businesses, unless that business is directly related to the school, and express permission has been sought and given by the Headteacher;
- use any USB external devices on the School Network without prior permission from the IT Infrastructure Manager. If permission is given, these devices must be virus checked by Eduthing before connection;
- use any external devices (including external USB storage devices) to store School related child or adult personal information;
- take or store images of present or past pupils of the School on personal Mobile Technology;
- access any personal Mobile Technology while in the vicinity of any children. All personal Mobile Technology must be kept out of sight in a pocket or bag when children are present. I understand that I will be challenged if I do not adhere to this rule.

I will:

- take all reasonable steps to protect the School Network including locking any devices I am logged into when I am away from the screen (⊞+L);
- always use the School Network and internet responsibly, and ensure that pupils in my care do so too;
- only use the School Network and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

- only use my School O365 OneDrive cloud storage for any School related external storage needs.
- 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.
- let the OLS Lead and Designated Safeguarding Lead (DSL) know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.
- ensure that all electronic communications with pupils and staff are compatible with my professional role and the guidance given in the OLS Policy.
- ONLY use the approved Microsoft Outlook mail system and my School issued email account or appropriate shared mailbox (i.e. Year Group email accounts) for School business.
- ensure that School Personal Information relating to children or adults is kept secure and is used appropriately, whether in School, taken off the School premises via cloud storage or accessed remotely. Personal Information can only be taken out of School or accessed remotely as a necessary part of my professional role.
- ensure that images of pupils and/or staff will only be taken, stored and used for professional purposes in line with School policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the School Network without the permission of the parent/carer, member of staff or Headteacher.
- store all images in the Media folder on the S drive.
- respect copyright and intellectual property rights.
- support and promote the School's Online Safety Policy and help pupils to be safe and responsible in their use of technology.
- ensure that all my use of School Network and personal devices, including, but not limited to, computers, cameras, tablets, Mobile Technology and any other internet-enabled device, complies with the School Online Safety policy.

Online Safety and Use of Images on Trips and Residential Visits

In addition to the points above, section 11.4.1 of the Online Safety Policy must be followed and acknowledged:

11.4.1 Parents/carers or volunteers supervising on school trips, residential visits, clubs or events **must not**:

- use their personal Mobile Technology when children are present;
- use their personal Mobile Technology to take photos or recordings of pupils, their work, or anything else which could identify a pupil;

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the School Business Manager, my Line Manager or Headteacher.

I understand and agree to abide by this AUA and to support the safe use of technology throughout the School.

Full Name of staff member /governor /contractor /volunteer /visitor:

_____

Job title / Company: _____

Signature: _____ **Date:** _____

Appendix 4: Parent/Carer Use of Images, Recordings and Work Consent Form and OLS Policy Agreement

PARENT/CARER CONSENT

St. Paul's Dorking
Church of England (Aided) Primary School

All pupils use computer facilities, the School Network and Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign an AUA (acceptable use agreement) to show that the Online Safety Rules have been understood and agreed.

Additionally, please review and complete the **Use of Images, Recordings and Work Consent Form** and **Online Safety Policy Agreement** below.

Parent/Carer name: _____

Pupil name: _____

PARENT/CARER CONSENT FOR USE OF IMAGES, RECORDINGS AND WORK

I AGREE / DO NOT AGREE (*please delete as appropriate*) that my son/daughter's **work** may be electronically published.

I AGREE / DO NOT AGREE (*please delete as appropriate*) that appropriate images and video that include my son/daughter **may be published**, subject to the School rule that photographs will not be accompanied by pupil names, as detailed in the Online Safety Policy. Images may be published, for example, in School Newsletters, in trip or sports event reports, on news pages on the Website or generally on the Website or in promotional materials.

Parent/Carer signature: _____ **Date:** _____

ONLINE SAFETY POLICY AGREEMENT

As the parent or legal guardian of the above pupil, I have read and understood the Online Safety Policy and Rules and Guidance in the Acceptable Use Agreement and grant permission for my daughter or son to have access to the School Network including the Internet and Teams learning platform.

I know that my son/daughter has signed an Online Safety Agreement form and that they have a copy of the Acceptable Use Agreement. We have discussed this document and my son/daughter agrees to follow the rules set out in the AUA and to support the safe and responsible use of the School Network at St Paul's CofE (Aided) School.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the School Network and internet, but I understand that the School will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the School can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their Online Safety or online behaviour that they will contact me.

I understand the School is not liable for any damages arising from my child's use of the Internet facilities.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my child's Online Safety.

Parent/Carer signature: _____ **Date:** _____

Please complete, sign and return to the School office.

Appendix 5: Staff Device/Laptop Loan Agreement

St. Paul's Dorking
Church of England (Aided) Primary School

STAFF DEVICE/LAPTOP LOAN AGREEMENT

Device Make: _____

Model: _____

Serial Number: _____

Date: _____

The laptop/device detailed above is loaned to _____ for the duration of their employment at the School subject to the following terms and conditions.

1. The laptop/device must be returned to the School when the member of staff ceases to be employed at the School, if required during a planned absence or if requested to do so by either the Headteacher or the ITIM.
2. The laptop/device is for the work-related use of the named member of staff to which it is issued.
3. Only software installed at the time of issue or software purchased by and licensed to the School may be installed on the machine.
4. The laptop/device remains the property of the School throughout the loan period. However, the member of staff to which it is issued, will be required to take responsibility for its care and safe keeping.
5. Should the equipment be lost or damaged due to the member of staff's lack of care or due to avoidable damage, it will be replaced or arrangement should be made for the repair of the equipment at the staff member's expense.
6. The laptop/device should not be left unattended and should be secured in a locked room or secure area. If left unattended for a short period in a car it must be placed in a locked boot out of sight.
7. Due regard must be given to the security of the laptop/device if using other forms of transport.
8. The laptop/device must be protected by a strong password containing at least 8 characters, including at least one uppercase letter, one lowercase letter, one number and one symbol.
9. In order to ensure the School's compliance with the Data Protection Act/ GDPR and to avoid breaches of confidentiality, under no circumstances should students be allowed to use staff laptops/devices. Staff should also be cautious when using the laptop/device away from School to ensure access is not given to files which may contain personal student data.
10. No School Data should be stored locally and all data must be stored on the School Network via the Remote Server or on a School O365 One Drive.
11. The laptop/device will be recalled from time to time for maintenance / upgrade and monitoring.
12. The equipment must be used in accordance with the School's Acceptable Use Agreement (AUA), Online Safety Policy, Safeguarding Policy, Data Protection Policy and Computing Policy.

I agree to the above conditions:

_____ Signature: _____ Date:_____

(*Print name*)

Returned:

_____ Date:_____

(**Signature of ITIM/ITTech**)

Appendix 6: Pupil Device/Laptop Loan Agreement

St. Paul's Dorking
Church of England (Aided) Primary School

PUPIL DEVICE/LAPTOP LOAN AGREEMENT

Device Make: _____

Model: _____

Serial Number: _____

Asset Tag Number: _____

Additional equipment issued with the device (i.e. power cords, cases etc): _____

_____

Pupil's Full Name: _____

Parent/Carer's Full Name: _____

Address: _____

_____

The laptop/device detailed above is jointly loaned to the pupil and parent/carer detailed above for the duration of the pupil's enrolment in the School, or until its return is requested by the School, and is subject to the following terms and conditions.

This agreement is between:

1) **St Paul's Church of England (Aided) Primary School** ("**the School**")
2) [Name of parent/carer(s)] ("**the parent**" and "**I**")

and governs the use and care of devices loaned to the child of the parent detailed above (the "**pupil**"). This agreement covers the period from the date the device is issued through to the return date of the device to the School (see below). All issued equipment shall remain the sole property of the School.

The School is lending the pupil a device (including all listed sundries) ("**the equipment**"), as detailed above, for the purpose of doing schoolwork from home. This agreement sets the conditions for taking the equipment home.

1 Damage/loss

By signing this agreement, I agree to take full responsibility for the equipment issued to the pupil and I have read, or heard this agreement read aloud, and understand the conditions of the agreement. I understand that I and the pupil are responsible for the equipment at all times.

If the equipment is damaged, lost or stolen, I will immediately inform the School (info@stpauls-dorking.surrey.sch.uk), and I acknowledge that I am responsible for the reasonable costs requested by the School to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police and advise the School of the police report reference number.

I agree to keep the equipment in good condition and to return it to the School on demand from the School in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

If the equipment is damaged, lost or stolen, and your child is eligible for the pupil premium or free school meals, please contact info@stpauls-dorking.surrey.sch.uk for advice.

I will make sure my child takes the following measures to protect the equipment:

- Keep the equipment in a secure place when not in use
- Not leave the equipment in a car or on show at home
- Not eat or drink around the equipment
- Not lend the equipment to siblings or friends
- Not leave the equipment unsupervised in unsecured areas

2 Acceptable use

I am aware that the School monitors the pupil's activity on this equipment.

Only software installed at the time of issue or software purchased by and licensed to the School may be installed on the equipment.

The equipment will be recalled from time to time for maintenance, upgrade and monitoring.

I agree that my child will not carry out any activity that constitutes 'unacceptable use' and will adhere to the guidelines as set out in the School's Online Safety Policy, Safeguarding Policy and Computing Policy.

This includes, but is not limited to, the following:

- Using the equipment or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Causing intentional damage to the equipment, other technology or materials
- Using inappropriate or offensive language

I accept that the School will sanction the pupil, in line with our Behaviour Policy, and this Loan Agreement will be terminated, if the pupil engages in any behaviour which constitutes unacceptable use.

3 Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

4 Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected – this password will be set by the School and must not be changed.
- Make sure my child locks the equipment if it is left inactive for a period of time
- Return the equipment to the School to enable updates to antivirus and anti-spyware software as required or updates to operating systems, as prompted

5 Return date

I will return the equipment in its original condition, and with all power cords and cases, to the School Office within 14 days of being requested to do so.

I will ensure the return of the equipment to the School immediately the pupil no longer attends the School.

6 Consent

I confirm that I have read the terms and conditions set out in this loan agreement and my signature below agreement confirms that I and the pupil will adhere to the terms of loan.

I agree to the above conditions:

_____ Signature: _____ Date:_____

(*Print name*)

Returned:

_____ Date: _____

(**Signature of ITIM/ITTech**)

Appendix 7: Online Safety Training Needs – self-audit for staff

St. Paul's Dorking
Church of England (Aided) Primary School

ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF	
Name of staff member/volunteer:	**Date**:
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the School's Acceptable Use Agreement for staff, contractors, volunteers, governors and visitors?	
Are you familiar with the school's Acceptable Use Agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the School's Network?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	