Abel Smith School Established 1861

Online Safety

Ownership:	Full Governing Body
Date of Issue:	April 2020
Review Date:	April 2021
Headteacher:	Daniel Hewitt
Signature:	
Date:	April 2020
Chair of Governors:	Katy Kay
Signature:	
Date:	April 2020

Policy Review

This policy will be reviewed in full by the Governing Body no less than annually.

The policy was last reviewed in May 2008 and was ratified by the Governing Body at the Full Governing Body meeting.

This policy has been updated on 17th April 2020 following the introduction of Government enforced social distancing rules, due the COVID-19 pandemic. The Governing Body ratified this policy remotely via Governor Hub on [date to be entered on ratification]

The next planned review is in April 2021.

Content

1. Introduction

Abel Smith school recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2019) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

This policy operates in conjunction with the following school policies:

- Child Protection
- GDPR
- Health and Safety
- Home School Agreement
- Positive Behaviour for Learning

- Anti-Bullying
- RSHE
- Social Media Policy

3. Roles and responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

3.1 The Governing Body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

3.2 The Headteacher is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

3.3 The Designated Senior Person (DSP) is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing body to update this policy on an annual basis.

3.4 IT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

3.5 All Staff Members are responsible for:

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

3.6 Parents and Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3.7 Outside organisations

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

4. Scope of Policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers

- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community and is supported by other school policies named in section two of this policy.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

Online safety is particularly addressed in the following subjects:

- RSHE / PSHE (Jigsaw)
- Computing

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. The schools approach to online safety is developed in line with the UK Council for Child Internet safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught underpinning knowledge and behaviours that can help them navigate the online world safely and confidently regardless of the device, platform or app they are using. They are encouraged to recognise the creative, collaborative, cultural, economic and educational opportunities provided such devices.
Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

The DSP is involved with the development of the school's online safety curriculum.

Abel Smith School recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSP will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSP will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

6. Policy and Procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or GovernorHub for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes.

Where required parent/carer permission will be obtained for the account to exist and the relevant acceptable use agreement has been completed. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Headteacher.

Any email that contains sensitive or personal information is only sent using the approved HCC secure and encrypted email system.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying). Teachers are also asked to maintain an appropriate conduct as set out by the teaching standards.

An annual assembly where they explain what a phishing email and other malicious emails might look like. This assembly includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.
- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect
- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Headteacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's acceptable use agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of Personal Mobile Devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device, unless there are extenuating circumstances and it has been agreed in advance by the Headteacher. When this is the case teachers are encouraged to remove their caller ID to protect their personal telephone number.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils in year 6 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. All such devices must be switched off and stored in their lockers. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Members of staff are permitted to access school emails and other collaboration applications. This permission is given by the Headteacher. Members of staff are required to ensure that their personal device is password protected, and that individual applications are also password protected. Password protection can take the form of pin code, fingerprint or face recognition.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Personal devices to take photos or videos of pupils and concerns about colleague use of personal devices on the school premises should be reported to the Headteacher.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with school policy.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSP.

Use of school-owned Devices

Some staff members are issued with the following devices to assist with their work:

- Laptop
- iPad

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

School-owned devices are used in accordance with the Device User Agreement.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks unless it has been agreed by the Headteacher and logged.

All school-owned devices are password protected.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

IT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from IT technicians.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

New Technological Devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher before they are brought into school.

7. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's acceptable use agreement as part of their induction and before having contact with pupils.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the acceptable use agreement (Appendix 2).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the acceptable use agreement (Appendix 3).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix 4).

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated annually and is delivered in line with advice from HCC and other online safety organisations. In addition to this training, staff also receive regular online safety updates as required.

The DSP and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.
- Act as the first point of contact for staff requiring advice about online safety.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

8. Working in Partnership with Parents and Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the acceptable use agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix 6. The acceptable use agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

9. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the acceptable use agreement. A record is kept of users who have been granted internet access.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

10. Social Networking

Personal Use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. Staff receive annual training on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSP and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

11. The School Website

The headteacher is responsible for the overall content of the school website and will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the Photography Policy are met.

12. Filtering and Monitoring Online Activity

The governing board ensures the school's IT network has appropriate filters and monitoring systems in place achieved by the Headteacher and IT technicians undertaking a risk assessment to determine what filtering and monitoring systems are required.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

IT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate. Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, IT technicians and the DSP will conduct a risk assessment. Any changes made to the system are recorded by IT technicians.

Reports of inappropriate websites or materials are made to an DSP immediately, who investigates the matter and makes any necessary changes. Deliberate breaches of the filtering system are reported to the Headteacher, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, appropriate action will be taken in line with the Behavioural Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored and All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the DSP who manages the situation in line with sections 15 and 16 of this policy.

Parents and carers are asked to carefully consider their home filtering systems and are encouraged to contact their service provider should they wish to make greater use their home internet filtering system.

13. Network Security

The following process are in place to ensure the school network remains safe and secure:

- Technical security features, such as anti-virus software, are kept up-to-date and managed by IT technicians and firewalls will be switched on at all times.
- IT technicians review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.
- Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- Staff members and pupils report all malware and virus attacks to ICT technicians.
- All members of staff have their own unique usernames and private passwords to access the school's systems.
- Pupils in class year or key stage and above are provided with their own unique username and private passwords, when required or needed.
- Staff members and pupils are responsible for keeping their passwords private.
- Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.
- Users are required to lock access to devices and systems when they are not in use.
- Users inform IT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.
- If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

14. Cloud Based Systems that Support Providing Education Remotely

Abel Smith School will be moving to a cloud based system that allows it to provide and deliver education remotely. Any cloud based system the school uses will enable student engagement. Teachers can empower pupil to create, reflect, share, and collaborate. Pupils "show what they know" using photos, videos, drawings, text, PDFs, and links both at school and at home.

Any cloud based system the school uses will require parental consent to ensure that parents are informed and in control of their child's information. GDPR also requires the school to seek parental consent before Seesaw can be used with pupils.

For further information on the school cloud based system please see Appendix 12, 13, 14

Please also see the school 'child protection policy, appendix 5, section 15' which gives further details of how the school is doing what it reasonability can to keep all our children safe whilst away from school.

Appendix 11 highlights the twenty considerations the school will make when delivering virtual lessons. Because we are supporting students remotely and sending work home does NOT mean that we will provide livestream lessons. Live streaming will only take place under very stringent circumstances and only by the expressed permission of the Headteacher. Where webcams are involved, the school and parents will ensure that:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by Abel Smith School to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held.

15. Managing Reports of Online Safety Incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies.

Concerns regarding a pupil's online behaviour are reported to the DSP who investigates concerns with relevant staff members. Pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature.

Where there is a concern that illegal activity has taken place, the Headteacher will contact the police.

All online safety incidents and the school's response are recorded by the DSP.

Section 16 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

16. Responding to Specific Online Safety Concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSP who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school. Incidents of upskirting are reported to the Headteacher who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal. All concerns regarding sexting are reported to the DSP.

Following a report of sexting, the following process is followed:

- The DSP holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so. If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the Headteacher first. The decision to view imagery is based on the professional judgement of the DSP and always complies with the Child Protection and Safeguarding Policy. Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded. If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it. The school will respond to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSP and dealt with in line with the Child Protection Policy.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved.

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

17. Records, Monitoring and Review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis and any changes are communicated to all members of the school community.

Online Harms and Risks – Curriculum Coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about.

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s):

	- Disinformation and why individuals or groups choose to share false information in order to deliberately deceive - Misinformation and being aware that false and misleading information can be shared inadvertently - Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons - That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online - How to measure and check authenticity online - The potential consequences of sharing information that may not be true	- RSHE (Jigsaw) - **[KS2 and above]** Computing curriculum
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: - How to recognise fake URLs and websites - What secure markings on websites are and how to assess the sources of emails - The risks of entering information to a website which is not secure - What pupils should do if they are harmed/targeted/groomed as a result of interacting with a fake website or scam email - Who pupils should go to for support	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw) - Computing curriculum
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: - What identity fraud, scams and phishing are - That children are sometimes targeted to access adults' data - What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw) - Computing curriculum
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s):

	• Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	• RSHE (Jigsaw) • Computing curriculum
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum

Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw)

	- The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges	
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: - That online content (sometimes gang related) can glamorise the possession of weapons and drugs - That to intentionally encourage or assist in an offence is also a criminal offence - How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw)
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: - That, in some cases, profiles may be people posing as someone they are not or may be 'bots' - How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw) - Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines). Teaching includes the following: - Boundaries in friendships with peers, in families, and with others - Key indicators of grooming behaviour - The importance of disengaging from contact with suspected grooming and telling a trusted adult - How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw)
Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s): - RSHE (Jigsaw)

	• What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	This risk or harm is covered in the following curriculum area(s): • Although this is not explicitly covered in any area of the curriculum we will sensitively support children in their understanding of an accurate portrayal of adult relationships.
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing curriculum

	• The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw)
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw)

Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw)
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): • RSHE (Jigsaw) • Computing Curriculum
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Online Safety Acceptable Use Agreement – Staff, Governors and Student Teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. Schools may wish to add further constraints regarding contact with former pupils, e.g. giving consideration to ex-pupils who are also known to be 'vulnerable' young people up to the age of 25.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. Student Teachers will be given a login by the IT Technician and agreement of the Headteacher.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I am able access secure school information from personal devices but I am required to ensure that my personal device is password protected, and that individual applications are also password protected. Password protection can take the form of pin code, fingerprint or face recognition.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSP or the Headteacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature: .... **Date:** ....

Full Name: .... (printed)

Job title: ....

Online Safety Acceptable Use Agreement – Peripatetic Teachers / Coaches, Supply Teachers

School Name: Abel Smith School

Online Safety Lead: Mr Daniel Hewitt

Designated Safeguarding Person (DSP): Mr Daniel Hewitt, Mrs Anna Cockley, Mrs Loraine Daniels (EYFS)

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social network accounts operated by the school. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device should be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP or the Headteacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature: .... **Date:** ....

Full Name: .... (printed)

Job title: ....

Appendix 4

Requirements for Visitors, Volunteers and Parent / Carer Helpers (working directly with children or otherwise)

School Name: Abel Smith School

Online Safety Lead: Mr Daniel Hewitt

Designated Safeguarding Person (DSP): Mr Daniel Hewitt, Mrs Anna Cockley, Mrs Loraine Daniels (EYFS)

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise any safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix 5

Online Safety Acceptable Use Agreement (Pupils / Parents)

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Abel Smith School Established 1861

Abel Smith School
Churchfields, Greencoates, Hertford
Hertfordshire. SG13 8AE
Tel: 01992 583 244
Email: admin@abelsmith.herts.sch.uk

Headteacher: Mr Daniel Hewitt

[Date]

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with your class teacher.

Please return the signed sections of this form which will be kept on record at the school.

Pupil Agreement

Pupil Name: ....

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil Signature: ....

Parent(s)/Carer(s) Agreement

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent / Carers Name(s): ....

Signature: .... Date: ....

Online Safety Policy Guide – Summary of key Parent / Carer Responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix 7

Guidance on the Process of Responding to Cyberbullying Incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Guidance for Staff on Preventing and Responding to Negative Comments on Social Media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix 6 (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Online Safety Incident Reporting Form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident, please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the Headteacher.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?	□	Outside school?	□
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?

Full names and/or contact details	
Children/young people:	
Staff member(s):	
Parent(s)/carer(s):	
Other, please specify:	

Type of incident(s) (indicate as many as apply)

Accessing age inappropriate websites, apps and social media	□	Accessing someone else's account without permission	□
Forwarding/spreading chain messages or threatening material	□	Posting images without permission of all involved	□
Online bullying or harassment (cyber bullying)	□	Posting material that will bring an individual or the school into disrepute	□
Racist, sexist, homophobic, religious or other hate material	□	Online gambling	□
Sexting/Child abuse images	□	Deliberately bypassing security	□
Grooming	□	Hacking or spreading viruses	□
Accessing, sharing or creating pornographic images and media	□	Accessing and/or sharing terrorist material	□
Accessing, sharing or creating violent images and media	□	Drug/bomb making material	□
Creating an account in someone else's name to bring them into disrepute	□	Breaching copyright regulations	□
Other breach of acceptable use agreement, please specify:			

Full description of the incident *What, when, where, how?*	
Name all social media involved *Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc*	
Evidence of the incident Specify any evidence available but do not attach.	

Thank you for completing and submitting this form.

OFFICE USE ONLY	
Immediate action taken following the reported incident:	
Incident reported to online safety Coordinator/DSL/ DSP/Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	
Brief summary of incident, investigation and outcome (for monitoring purposes)	

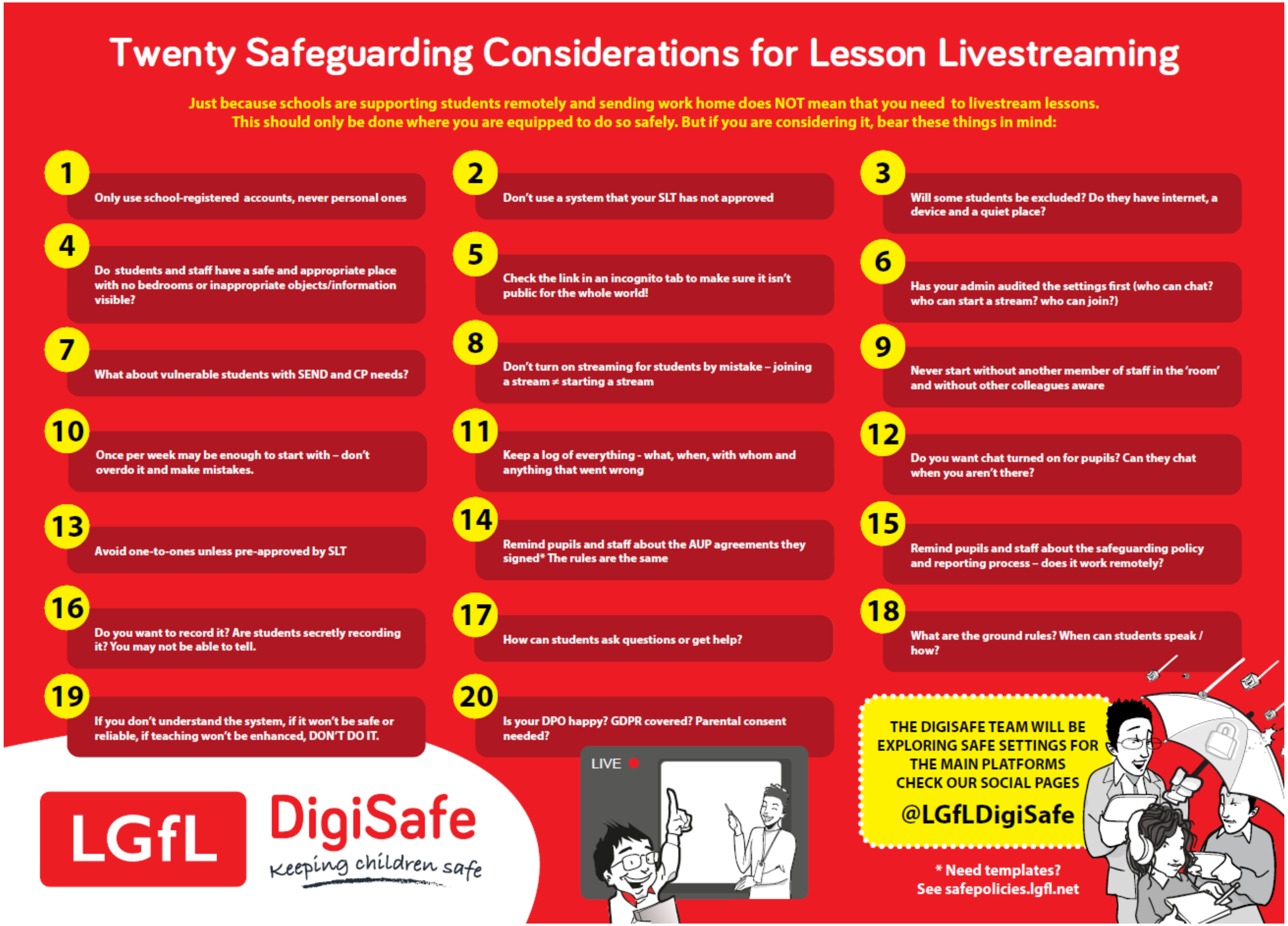
Appendix 10

Online Safety Incident Log

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

Safeguarding Consideration for Livestreaming and Virtual Lessons



Twenty Safeguarding Considerations for Lesson Livestreaming

Just because schools are supporting students remotely and sending work home does NOT mean that you need to livestream lessons. This should only be done where you are equipped to do so safely. But if you are considering it, bear these things in mind:

1 Only use school-registered accounts, never personal ones

2 Don't use a system that your SLT has not approved

3 Will some students be excluded? Do they have internet, a device and a quiet place?

4 Do students and staff have a safe and appropriate place with no bedrooms or inappropriate objects/information visible?

5 Check the link in an incognito tab to make sure it isn't public for the whole world!

6 Has your admin audited the settings first (who can chat? who can start a stream? who can join?)

7 What about vulnerable students with SEND and CP needs?

8 Don't turn on streaming for students by mistake – joining a stream ≠ starting a stream

9 Never start without another member of staff in the 'room' and without other colleagues aware

10 Once per week may be enough to start with – don't overdo it and make mistakes.

11 Keep a log of everything - what, when, with whom and anything that went wrong

12 Do you want chat turned on for pupils? Can they chat when you aren't there?

13 Avoid one-to-ones unless pre-approved by SLT

14 Remind pupils and staff about the AUP agreements they signed* The rules are the same

15 Remind pupils and staff about the safeguarding policy and reporting process – does it work remotely?

16 Do you want to record it? Are students secretly recording it? You may not be able to tell.

17 How can students ask questions or get help?

18 What are the ground rules? When can students speak / how?

19 If you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.

20 Is your DPO happy? GDPR covered? Parental consent needed?

LGfL DigiSafe

Keeping children safe

THE DIGISAFE TEAM WILL BE EXPLORING SAFE SETTINGS FOR THE MAIN PLATFORMS CHECK OUR SOCIAL PAGES

@LGfLDigiSafe

* Need templates?
See safepolicies.lgfl.net

Appendix 12

Abel Smith School Cloud Based Learning System – Seesaw

What is Seesaw?

Seesaw is a platform for student engagement. Teachers can empower students to create, reflect, share, and collaborate. Students "show what they know" using photos, videos, drawings, text, PDFs, and links. It's simple to get student work in one place and share with families, and nothing is shared without teacher approval.

Trust and Safety

How does Seesaw help keep student data safe?

Seesaw takes protecting your security and privacy seriously and we've put a number of measures in place to protect the integrity of your information.

- Seesaw has a robust set of Privacy Principles designed to clearly communicate privacy promises to our teachers, families and students.
- Seesaw uses TLS 1.2 security at the network level to ensure all account information and journal content is transmitted securely.
- Journal Content (e.g., the photos, video, audio, and other content you add to your Seesaw journal) is encrypted at rest.
- All passwords are salted and hashed using PBKDF2.
- Seesaw routinely conducts 3rd party security audits to verify the security and integrity of our systems and internal controls.
- Data is stored in access-controlled data centres operated by industry leading partners with years of experience in large-scale data centres with 24/7 monitoring.
- All user information is stored redundantly and backed up in geographically distributed data centres. Seesaw utilise multiple distributed servers to ensure high levels of uptime and to ensure that they can restore availability and access to personal data in a timely manner.
- Seesaw have adopted an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support).
- All employees undergo a background check before beginning employment at Seesaw, sign a nondisclosure agreement, and immediately lose access to all internal systems and data when terminated. No customer information is stored on individual employee computers.
- Seesaw routinely monitor their systems for security breaches and attempts at inappropriate access.
- Seesaw use encrypted QR codes for family and student access to journal content.
- Seesaw has taken the Student Privacy Pledge.
- Seesaw complies with the EU - U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries. Seesaw has certified that it adheres to the Privacy Shield Privacy Principles of notice, choice, accountability for onward transfer, security, data integrity, access, and enforcement and liability. You can learn more about the Privacy Shield program on their website, or view our certification page here.

Where is my data stored?

Seesaw contracts with Amazon Web Services (AWS) to provide data centre and server hosting services for Seesaw - this means things like making sure the Seesaw servers are always on and fast regardless where in the world you are accessing Seesaw. Amazon has robust security practices and is contractually prohibited from using any personal information that is stored on servers they operate for any purpose other than to operate the Seesaw service.

Seesaw take student data privacy extremely seriously. You can learn more in our Privacy Policy and How Seesaw Keep Student Information Safe. By default, your data is stored in the United States. If Abel Smith School decides to purchased Seesaw for Schools, it can opt to store all data associated with the school in another region such as Canada, Australia, or the EU.

Seesaw also complies with the EU-U.S. Privacy Shield Framework. Seesaw has certified that it adheres to the Privacy Shield Privacy Principles of notice, choice, accountability for onward transfer, security, data integrity, access, and enforcement and liability. You can learn more about the Privacy Shield program on their website, or view Seesaw certification page here.

Who can view student journals?

Seesaw journals are private by default. No student content or information is ever shared without your explicit request.

Journals are only accessible to teachers, students in the class, and a student's family if the teacher chooses to invite them.

Links to Seesaw journal posts can only be accessed if shared by a teacher, family, or student account. Links are not searchable.

Family members are only able to access their own child's journal, not the journals of other students in the class.

If a family member is still concerned about their child's privacy, you can observe these guidelines for that child:

- Do not post group photos that include the child
- Do not tag the child in posts that include any other members of the class.
- Only invite the child's primary family to view their journal and do not invite other family members
- Refrain from posting photos of the child, and instead focus on photos of their school work
- Do not post that child's work to the blog (if you have turned on the blog for your class)

Family sharing can be turned off class settings. When family sharing is disabled, families will not have the ability to download any posts onto their device or share any posts over social media. They can of course, take a screenshot which unfortunately in impossible to control.

Why do I have to verify my email and add my school?

Seesaw is designed for educational use. Seesaw ask emails to be verified and schools to be confirmed to ensure Seesaw is being used in an educational setting. This information also helps look up account information if customer support is needed.

Where can I find Seesaw's ICO Supplier Self Certification Statement?

You can access Seesaw's self-certification statement here.

GDPR

Yes, Seesaw is GDPR compliant.

What is Seesaw doing to comply with GDPR?

The principles of privacy by design and privacy by default outlined in the GDPR have been core to the Seesaw mission, experience and product development process from the beginning. We have a number of tools and options in place today to protect the integrity of teachers, students and families' information globally.

These tools for control and transparency address many of the goals of the GDPR today and are outlined below, along with some additional updates we are making.

Tools for Control

In Seesaw today you can do the following to get information about, access, rectify or erase your personal data - all rights outlined in the GDPR.

- You can update your Seesaw account settings at any time to correct or complete your account information.
- Students can export their journals at any time from their Seesaw account.
- You can delete your Seesaw account at any time and we will permanently delete your account and all data associated with it within 60 days.

Additional tools that put you in control address the right outlined in the GDPR to object to how your data is being used:

- We provide tools to help teachers get parental consent to use Seesaw in their classrooms.
- Furthermore, we do not use personal data in any advertising and do not sell any user data.

Transparency

Seesaw is also committed to transparent policies.

Our Privacy Policy describes what data we collect and how we use it.

Our longstanding Privacy Principles summarize our privacy commitments to you.

If anything substantial changes with our privacy practices, we'll let you know. The privacy policy and terms you agreed to will still apply unless you accept the new terms.

If you have specific questions about particular data, you can contact privacy@seesaw.me.

Beyond these existing practices, we are doing the following to meet **additional needs of the GDPR:**

- We reviewed our contracts with third party vendors to make sure that they are compliant with the GDPR.
- We delivered GDPR-focused security training to Seesaw employees.
- We strengthened our procedures for data subject access requests, deletion requests, and government access requests.
- We appointed a Data Protection Officer.
- We implemented a Data Protection Impact Assessment process.

Does GDPR require storage of personal data in the EU?

No, GDPR does not require storage of personal data in the EU. GDPR does have specific requirements regarding the transfer of data out of the EU, but these requirements are similar to existing EU law, which Seesaw complies with.

Privacy Shield is an agreement between the EU and US allowing for the transfer of personal data from the EU to US. Privacy Shield allows US companies to meet this requirement of the GDPR.

Seesaw complies with Privacy Shield regarding the collection, use and retention of personal information from European Union member countries. Seesaw has certified that it adheres to the Privacy Shield Privacy Principles of notice, choice, accountability for onward transfer, security, data integrity, access, and enforcement and liability. You can learn more about the Privacy Shield program on their website, or view our certification page here.

Seesaw also offers an optional service for Seesaw for Schools customers to have data stored outside the United States in Australia, Europe, United Kingdom, or Canada. Abel Smith School will work towards data storage being UK or EU based as soon as practically possible.

What responsibilities does Abel Smith School have?

Abel Smith School has a responsibility to comply with GDPR. Under GDPR Abel Smith School needs to get parental consent to process personal data for children under the age of 16. This consent is collected as part of a school wide consent that includes Seesaw.

Why does Abel Smith School need to get parental consent?

Getting parental consent helps ensure that parents are informed and in control of their child's information.

European Union privacy laws (known as the GDPR) and the Seesaw Terms of Service require that schools get parental consent before using Seesaw with students.

Protecting your privacy is fundamental to Seesaw's mission and business. For more information, you can read more about our privacy commitments and how we keep your information safe.

Does Seesaw offer a Data Processing Agreement?

Yes, Seesaw offers a Data Processing Agreement to schools located in the EU/EEA and Switzerland, in addition to their Privacy Policy and Privacy Principles. Abel Smith School has requested a Data Processing Agreement.

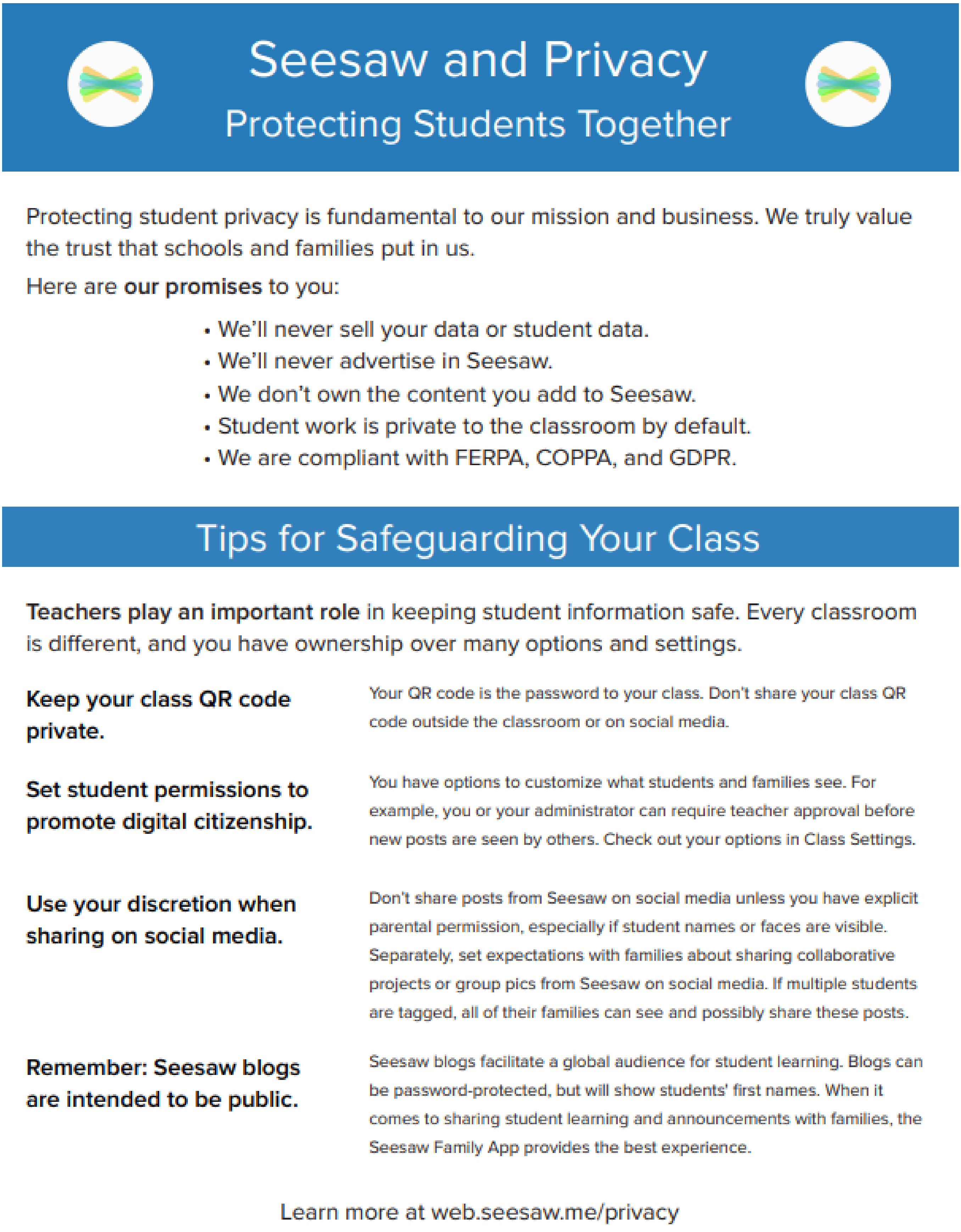
Who are Seesaw's sub-processors?

Seesaw uses a handful of third party sub-processors - other companies that provide software services that help us do business. These companies help Seesaw do things like manage their data centres to make sure Seesaw is reliable and fast or provide software that powers our customer support.

Seesaw's sub-processors have all signed a Data Protection Agreement with us, which stipulates that any data share with them will be used exclusively to provide services to Seesaw and not for any other purposes.

Currently Seesaw uses sub-processors to:

Host & Deliver Seesaw	Amazon Web Services (Data center management) LaunchDarkly (Beta testing support)	AWS Privacy Policy Launch Darkly Privacy Policy
Communicate with Teachers, Families, and Administrators	Autopilot (Sending emails) Boomerang (Sending emails) Mailchimp (Sending emails) Mailgun (Sending emails) Twilio (Sending text messages) Versal (Provide online courses)	Autopilot Privacy Policy Boomerang Privacy Policy Mailchimp Privacy Policy Mailgun Privacy Policy Twilio Privacy Policy Versal Privacy Policy
Run our Internal Operations	Zendesk (Software for customer support) Ada (Software for customer support) Shopify (Operating the Seesaw store) Salesforce (Manage customer relationships) Outreach (Organize communications with schools) Wufoo (Collect interest in Seesaw for Schools) Docusign (Electronically sign contracts with schools) SaaSOptics (Manage our internal finances) Quickbooks (Manage our internal finances) Survey Monkey (Conduct surveys and user research) Google (Manage emails, calendars, and documents)	Zendesk Privacy Policy Ada Privacy Policy Shopify Privacy Policy Salesforce Privacy Policy Outreach Privacy Policy Wufoo Privacy Policy Docusign Privacy Policy SaaSOptics Privacy Policy Quickbooks Privacy Policy Survey Monkey Privacy Policy Google Privacy Policy



Seesaw and Privacy

Protecting Students Together

Protecting student privacy is fundamental to our mission and business. We truly value the trust that schools and families put in us.

Here are **our promises** to you:

- We'll never sell your data or student data.
- We'll never advertise in Seesaw.
- We don't own the content you add to Seesaw.
- Student work is private to the classroom by default.
- We are compliant with FERPA, COPPA, and GDPR.

Tips for Safeguarding Your Class

Teachers play an important role in keeping student information safe. Every classroom is different, and you have ownership over many options and settings.

Keep your class QR code private.

Your QR code is the password to your class. Don't share your class QR code outside the classroom or on social media.

Set student permissions to promote digital citizenship.

You have options to customize what students and families see. For example, you or your administrator can require teacher approval before new posts are seen by others. Check out your options in Class Settings.

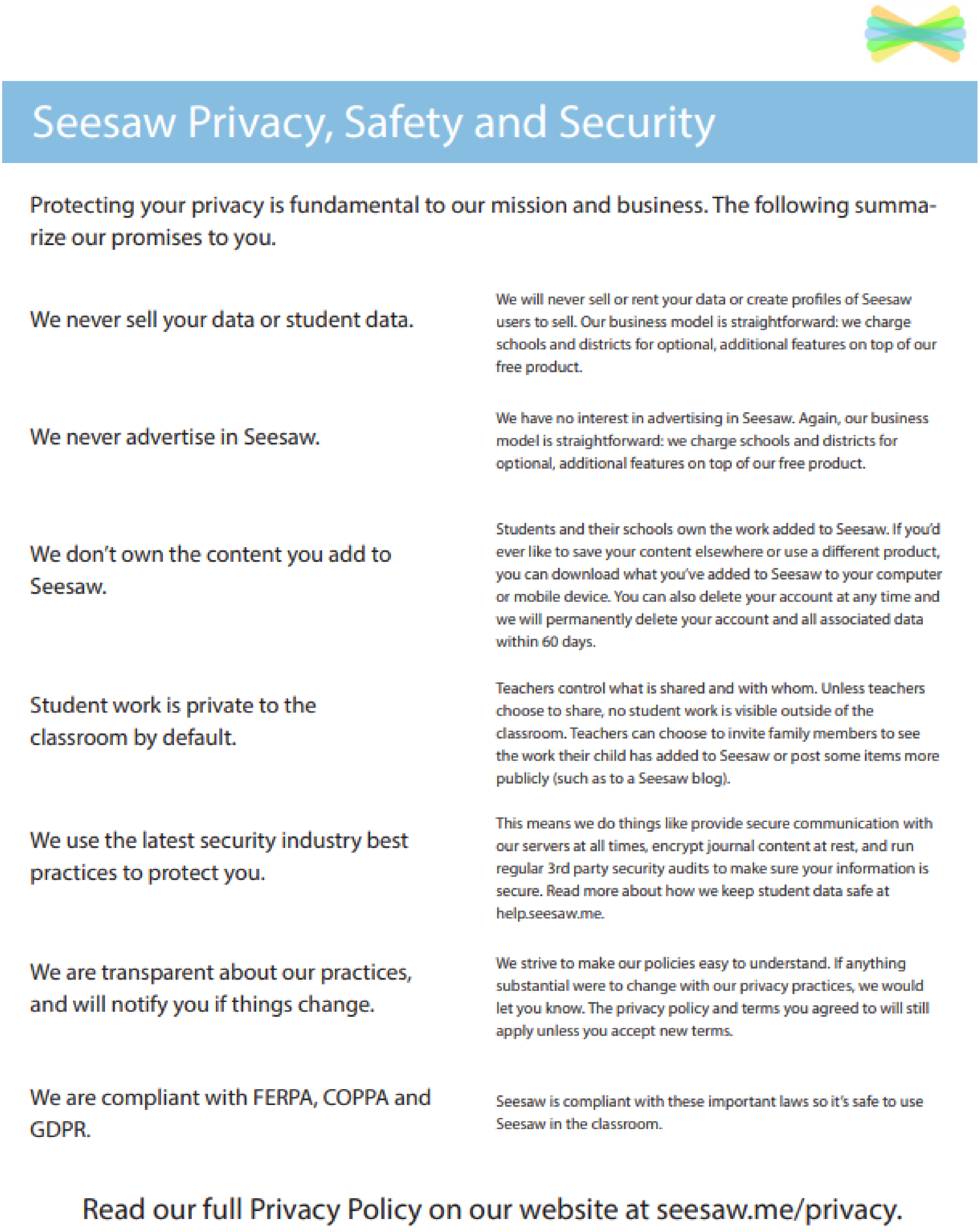
Use your discretion when sharing on social media.

Don't share posts from Seesaw on social media unless you have explicit parental permission, especially if student names or faces are visible. Separately, set expectations with families about sharing collaborative projects or group pics from Seesaw on social media. If multiple students are tagged, all of their families can see and possibly share these posts.

Remember: Seesaw blogs are intended to be public.

Seesaw blogs facilitate a global audience for student learning. Blogs can be password-protected, but will show students' first names. When it comes to sharing student learning and announcements with families, the Seesaw Family App provides the best experience.

Learn more at web.seesaw.me/privacy



Seesaw Privacy, Safety and Security

Protecting your privacy is fundamental to our mission and business. The following summarize our promises to you.

We never sell your data or student data.

We will never sell or rent your data or create profiles of Seesaw users to sell. Our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.

We never advertise in Seesaw.

We have no interest in advertising in Seesaw. Again, our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.

We don't own the content you add to Seesaw.

Students and their schools own the work added to Seesaw. If you'd ever like to save your content elsewhere or use a different product, you can download what you've added to Seesaw to your computer or mobile device. You can also delete your account at any time and we will permanently delete your account and all associated data within 60 days.

Student work is private to the classroom by default.

Teachers control what is shared and with whom. Unless teachers choose to share, no student work is visible outside of the classroom. Teachers can choose to invite family members to see the work their child has added to Seesaw or post some items more publicly (such as to a Seesaw blog).

We use the latest security industry best practices to protect you.

This means we do things like provide secure communication with our servers at all times, encrypt journal content at rest, and run regular 3rd party security audits to make sure your information is secure. Read more about how we keep student data safe at help.seesaw.me.

We are transparent about our practices, and will notify you if things change.

We strive to make our policies easy to understand. If anything substantial were to change with our privacy practices, we would let you know. The privacy policy and terms you agreed to will still apply unless you accept new terms.

We are compliant with FERPA, COPPA and GDPR.

Seesaw is compliant with these important laws so it's safe to use Seesaw in the classroom.

Read our full Privacy Policy on our website at seesaw.me/privacy.

Appendix 13

Abel Smith School EYFS Cloud Based Learning System – Evidence Me

1. What is Evidence Me?

Evidence Me (formerly 2Build a Profile (2BAP)) is an award-winning assessment, observation and reporting app developed by 2Simple Ltd. It shows the impact of children's learning by capturing learners' experiences, monitoring their development and creating reports to share their progress. The app has been thoughtfully created by teachers, for teachers and ensures all the essential features required have been included.

2. Personal Data and Data Processing Agreement

2.1 With regard to 2Simple Products, Abel Smith School is the Data Controller for the Purposes of Data Protection Legislation. This means that Abel Smith School are required to meet the statutory obligations with regard to the processing of personal data.

2.2 For the purposes of compliance with the legislation, the terms below set out how any data transferred from Abel Smith School to 2Simple will be handled.

2.3 It is expressly agreed between Abel Smith School and 2Simple that for the purposes of any contract where 2Simple are required to process data owned by the school:

2.4 The school shall remain the owner of any personal data which may be transferred to 2Simple under any contract between Abel Smith School and 2Simple.

2.5 2Simple shall act as a data processor for the processing of personal data on behalf of Abel Smith School.

2.6 By using our 2Simple Products Abel Smith School warrant that we have complied with all relevant data protection laws and obtained all relevant consents to the processing of the data stored in 2Simple Products and Abel Smith School are lawfully able to transfer such data to 2Simple. If such data is entered or stored in 2Simple Products by children within the school this will require informed consent from parents or guardians.

2.7 2Simple warrant that they shall:

- Only process the personal data for the purposes of the contract between 2Simple and Abel Smith School;
- Only use the personal data to comply with our obligations under that contract;
- Not transfer the data or any copy of the data outside the European Economic Area without the express prior written agreement from Abel Smith School;
- Maintain appropriate technical and organisational security measures against the unauthorised or unlawful processing of the personal data.
- Not subcontract any of our rights or obligations under this agreement without Abel Smith School's prior written consent.
- Where 2Simple consent subcontract any of Abel Smith School's obligations under a signed agreement, 2Simple shall do so only by way of a written agreement with the subcontractor that imposes the same obligations in relation to the security of the processing on the subcontractor as are imposed on 2Simple under a signed agreement.
- Take reasonable steps to ensure the reliability of any employees and ensure that those employees have received adequate data protection training.
- Report any breach of data to you within 48 hours.
- Comply with the Data Protection Act 2018 and the EU General Data Protection Regulation.

2.8 2Simple will at all times cooperate with Abel Smith School for monitoring and evaluating compliance with data protection legislation including allowing the school access to audit the security measures 2Simple have in place and personal data.

2.9 If Abel Smith School give 2Simple instructions that are, in the judgment of 2Simple, incompatible with the proper running of operations, 2Simple will be at liberty to refuse to continue to provide data processing services to Abel Smith School.

2.10 2Simple agree that they shall maintain the personal data processed by them on behalf of Abel Smith School in confidence. Subject to paragraph 2.11 below, 2Simple agree that, unless they have the schools prior written consent, they shall not disclose any personal data supplied to them to any third party except our authorised sub-processors operating under conditions of strict confidence.

2.11 Nothing in this agreement shall prevent either 2Simple or Abel Smith School complying with any legal obligation imposed by a regulator or court.

2.12 When the subscription has terminated 2Simple will cease all processing of personal data and delete such personal data or at the schools request and subject to a reasonable fee will return personal data to the school in an agreed format.

2.13 2Simple's full data Processing Agreement can be found here.

3. Data Deletion Policy

3.1 This policy applies to personal data, including usernames and saved work including blogs and emails within our Products (User Data). It also applies to templates and lesson plans published on our Products and other similar documents that have been shared or published on our Products for public consumption (Template Data).

3.2 User Data will be deleted from our system in the following circumstances:

(a) A written request is made by the account holder for deletion of the User Data. In these circumstances, we undertake to ensure its deletion within 2 (two) weeks of receiving such a request.

(b) An organisation's or individual user's subscription has ended, and 12 (twelve) months have elapsed.

(c) User Data has been placed in the trash bin for a period of 12 (twelve) months without being removed or restored by the user.

(d) User Data has been placed by the user in the software's trash bin and the user has selected "delete" and a further 12 (twelve) months have elapsed.

(e) An email request is made to our technical support team to update the pupil records for a school, and pupils who have

3.3 left the school are not included as current pupils. In such circumstances, pupils who have left the school and their associated data will be moved to the trash bin and dealt with in accordance with paragraph 6.2(c) above.

3.4 Once User Data has been deleted from our system in accordance with paragraph 3.2 above it will remain on our database backups for a period of up to 1 (one) month. Thereafter it will be permanently deleted.

3.5 Subject to the exception set out below, data that has been published on our Products to the general public for sharing (such as templates, lessons plans etc) will not be deleted in accordance with paragraph 3 above and will remain on systems until such time as a request is forthcoming from the creator of the Template Data that it should be deleted. On receipt of such a request, we undertake to remove it from our system within 2 (two) weeks, and for it to be deleted from system backups in a further month.

3.6 The exception to the rule at 3.4 is that if Template Data has been published in contravention of our guidelines (for instance in breach of copyright), we reserve the right to take it down and delete it earlier.

4. Privacy Notice

The information that Abel Smith School provides to 2Simple will only be used by 2Simple in accordance with its Privacy Notice. 2Simple use cookies on their site and by using their Products the school consent to the use of such cookies, full details of how 2Simple use them are contained within their Privacy Notice.

Please read the Privacy Notice carefully and if you have any questions please email support@2Simple.com.

5. GDPR

5.1 Yes, 2Simple (Evidence Me) is GDPR compliant.

5.2 By this statement 2Simple is seeking to inform employees, customers, business partners and suppliers of its commitment to good data protection practice and its ongoing GDPR compliance.

5.3 The EU General Data Protection Regulation (GDPR) becomes effective on 25 May 2018. The GDPR has brought considerable changes to data protection law both in the UK and across the European Economic Area.

5.4 2Simple has always sought to ensure compliance with data protection law and these practices have stood it in good stead in advance of GDPR.

5.5 In 2017 2Simple commenced a programme to ensure its compliance with GDPR. Further to this programme, 2Simple can now confirm that it has:

- An established privacy governance structure.
- Embedded GDPR requirements into policies and day-to-day activities.
- Implemented technical measures to ensure GDPR compliance.
- Documented and recorded compliance measures.
- Implemented internal training for GDPR compliance.
- Audited data protection measures with audit results used to implement compliance.

5.6 2Simple recognises that GDPR is new for many of its customers, business partners and suppliers who are modifying their own data protection practices and operations to ensure GDPR compliance and 2Simple will provide assistance with this wherever it can.

5.7 2Simple is also aware that GDPR provisions allow member states to enact new legislation specifying, restricting, or expanding the scope of the GDPR's requirements.

5.8 To respond to the needs of its customers, business partners and suppliers and any new legislation, 2Simple will keep its GDPR programme under review and will continue to provide updates of its data protection practices and compliance.

5.9 Should you have any questions about this statement, please contact our friendly customer support team at support@2simple.com.

Appendix 14

Abel Smith School Multiplication Cloud Based Learning System – TT Rock Stars

What is TT Rock Stars?

Times Tables Rock Stars is a carefully sequenced programme of daily times tables practice which children complete online using a personal device. Times Table Rocks Stars is produced by a company called Maths Circle Ltd. Times Tables Rock Stars is designed to boost times tables recall and maths confidence (comprising a website, app, worksheets and teacher resources).

You can read Maths Circle Ltd full privacy notice here.

Maths Circle Ltd Cookie Policy

A cookie is a little piece of information handed to a web browser from a web server that contains information that can be retrieved from the server later. When you visit the Sites the server may attach a cookie to your computer's memory. We use cookies only to remember what language is set, which school last logged into the machine and the session cookie for knowing who is logged in. You should be able to configure your browser so that it disables cookies.

To help us better understand your needs, we also use analytical software. This software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the Sites, but will not store, save or collect personal information.

How does Maths Circle Ltd keep our personal information secure?

Maths Circle Ltd use appropriate technical and organisational measures to protect the personal information they collect and process. The data that is collected is stored on secure servers in Germany. The measures used are designed to provide a level of security appropriate to the risk of processing personal information. All traffic and passwords are encrypted. As part of their privacy compliance processes, Maths Circle Ltd reviews these security procedures to consider appropriate new technology and methods.

International Data Transfers

Personal information may be transferred to, and processed in, countries other than the country in which we reside. These countries may have data protection laws that are different to the laws of your country. Specifically, Sites servers are located in Europe through Hertzner, Amazon Web Services and Heroku. However, Maths Circle Ltd have taken appropriate safeguards to require that your personal information will remain protected in accordance with their Privacy Notice.

Data Retention

Maths Circle Ltd retains personal information collected from Users where we have an ongoing legitimate business need to do so (for example, to provide a service you have requested or to comply with applicable legal, tax or accounting requirements).

When they have no ongoing legitimate business need to process User's personal information, or where they are asked to delete Users' information, they will take reasonable steps to either delete or anonymise it. If this is not possible immediately (for example, because your personal information has been stored in backup archives), then they will securely store Users' personal information and isolate it from any further processing until deletion is possible but will endeavour to do so as soon as reasonably practicable. Maths Circle Ltd may have to retain and use personal information as necessary to comply with legal and regulatory obligations, to resolve disputes, and to enforce our terms and conditions.

Their policy is to automatically delete all pupil/child data from school accounts, tutor accounts and family accounts 12 weeks after expiry of a free trial or expiry of a subscription, where no renewal or pending subscription has been requested by that school, tutor or family.

Maths Circle Ltd GDPR Statement

To the best of their knowledge, having sought legal advice, performed several audits and followed technical recommendations, Maths Circle are GDPR compliant. In order to remain so, they continually monitor changes in legislation and make amendments, should they need to, in light of these.

You can read Maths Circle Ltd GDPR – Commonly Asked Questions by clicking here.