E-Safety and Acceptable Use Policy

	Signature	Date
Chair of Committee		
Headteacher		
Committee Approval		Spring 2025
Next Review Date		Spring 2026

E-Safety and Acceptable Use Policy

Contents

E-Safety and Acceptable Use Policy

1. Introduction

Newtown School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. 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 supported 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 helping children and young people navigate the online world safely and confidently.

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Responsibilities

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, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their children 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. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, Health and Safety, Remote Learning, Behaviour and Anti-bullying policies.

2.1 Governors and Headteacher

The Headteacher and Governors have ultimate responsibility to ensure that appropriate Online Safety Policy and practice is embedded and monitored.
All breaches of this policy must be reported to the Headteacher.
All breaches of this policy that may have put a child at risk must also be reported to a DSL, Hayley England or Daniel Rose.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

2.2 The designated safeguarding lead (DSL)

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

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

2.3 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

2.4 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and reporting any failures of the system to the DSL
- Following the correct procedures by if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

2.5 Parents/carers

Parents/carers are expected to:

- Ensure they have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

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, cloud-based services and/or 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.

3. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, 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 for all official school 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 do not have access to emails on the school system. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the GDPR policy. 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.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to children. 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 and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have 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 content.
- When working with pupils searching for images should be done through Google Search, 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: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- 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

Users must not:

- 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.

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).

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. Staff and pupils may have temporary access to photographs taken during a school trips, but these will be transferred/deleted promptly.

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 children.

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 for 2 factor authentification. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device without the express permission of the Headteacher.

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 are **not** allowed to bring personal mobile devices/phones to school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

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.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSP, the Headteacher or Deputy Headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

4. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which sets the foundations for children to become informed, safe and responsible. Online Safety sits within the Newtown PSHE and Computing curriculum.

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

5. 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 and student teachers are provided with a copy of the Online Safety Policy and must sign the school's Acceptable Use Agreement as part of their induction. The Acceptable Use Agreement is in the staff handbook, which is emailed to all staff annually, available in the staffroom and on the staff drive.

Any organisation working with children and based on the school premises are also provided with a copy of the Online Safety Policy and required to sign the Acceptable Use Agreement, this is kept with their letting agreements.

Peripatetic staff, coaches and regular professional visitors are provided with a copy of the Online Safety Policy and are required to sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and parent/carer helpers.

6. Working in Partnership with Parents/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. The support of parents/carers is essential to implement the Online Safety Policy effectively and help keep children safe.

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, newsletters and by other means.

Parents/carers are asked on an annual basis to read and discuss the children's Acceptable Use Agreement. A summary of key parent/carer responsibilities along with further support and advice is also provided and is in the Parent Handbook which is emailed annually and on the school website.

7. 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 by the Headteacher (in the staff section of CPOMS). All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Staff will record any incidents involving children on CPOMS, this will automatically be flagged up with the Headteacher and Deputy Headteacher. Other breaches will be reported to the Headteacher who will deal with them appropriately, informing other agencies as necessary.

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 receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, 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.

Appendix 1

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, student teachers 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.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to support@ikon-ict.com

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 the 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, current pupils or ex-pupils of school age.

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.

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

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 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 will not access secure school information from personal devices when in school or any other location except through the Office 365 system.

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.

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 DSL 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. I will also check the appropriacy of any suggested sites suggested for remote learning. If I access inappropriate material, I will report this to the DSL and/or IKON.

Video conferencing
I will only use the conferencing tools that have been identified and risk assessed by the school leadership and DSL. A school-owned device should be used when running video-conferences, where possible.

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: ……

Appendix 2

Online Safety Acceptable Use Agreement
Peripatetic Teachers / Coaches / Regular Visiting Professionals

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 Peripatetic Teachers / Coaches / Regular Visiting Professionals 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, 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.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to support@ikon-ict.com

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 the 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, current pupils or ex-pupils of school age.

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.

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/DSP, or a young person's or parent/carer's own device.

Use of Email
I will only use my professional 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 could be used to access specialist apps that support pupil learning.

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 or during a tutoring session; 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 access inappropriate material, I will report this to the DSL and/or IKON.

Video conferencing
I will only use the conferencing tools that have been identified and risk assessed by the school. A school-owned device should be used when running video-conferences, where possible.

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 3

Online Safety Requirements for visitors, volunteers and parent/carer helpers
(Working directly with children or otherwise)

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 or Deputy Headteacher, both of whom are Designated Safeguarding Leads.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in the staff room. When not in the staff room, phones must be switched off and locked in a locker or handed in to the office. Any exception must be pre-arranged and agreed by the Headteacher or Deputy Headteacher.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any exception must be pre-arranged and agreed by the Headteacher or Deputy Headteacher.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP 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 on-line, 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.

Signature: …….. Date ……

Full Name: …….. (printed)

Appendix 4

Online Safety Acceptable Use Agreement for Pupils

Online Safety Rules

These are rules that the children will be expected to follow during their time at Newtown, they will be explained in age appropriate terms through our Safety and Wellbeing Curriculum.

- In school I will only use school IT equipment for activities agreed by school staff.
- In school I will only open or delete my files when told to by a member of staff.
- I understand that no personal devices are allowed in school, and I will follow the rules.
- I understand my behaviour in a school Teams meeting should mirror that in the physical classroom.
- If I come across anything online that is 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.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- Uploading or sending my image or other people's (photographs, videos, live streaming) online puts us at risk. I will always seek permission from my teacher or parent/carer if I wish to do this.
- 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 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.

It is important that parents/ carers also understand the expectations that they and their children are expected to follow during their time at Newtown. Further information for parents is on the next page. Please read both and then sign and return to the school office. A copy of the agreement is in the parent handbook that is sent out every academic year. If you have any concerns, please contact the Headteacher.

Parents/Carers agreement

Signature of parent: …… Date: ……

Full Name of parent: …… (printed)

Full Name of child: …… (printed) Class: ……

Appendix 5

Online Safety Policy - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website and via email. 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 the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may not use personal mobile phones and devices in 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, their phone/s must be switched off and out of sight.
- Parents/carers should know that pupils **cannot** bring any technological devices to school as per the school policy.
- Children under the age of 13 should not be on Facebook, Instagram or other social media sites. If the school finds out that children have accounts it will be regarding as a child protection concern and dealt with accordingly.
- Parents/carers have a responsibility to keep their children safe online whilst at home, this includes use of multiplayer internet based games on the X-Box or PlayStation where children can be at risk of grooming or contact with older children or inappropriate adults. Parents are expected to use parental controls and monitor children's activity.
- Online games, like films, have an age restriction. It is important that parents follow this guidance. If the school finds out that children have played inappropriate games, it will be regarding as a child protection concern and dealt with accordingly.
- 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. Further guidance and support are available from:

Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, Vlogging & livestreaming, online gaming and cyberbullying. www.internetmatters.org/

NSPCC - includes a range of resources to help parents keep children safe when they're using the internet, social networks, apps, games and more. www.nspcc.org.uk

Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents covering all of the issues amplified by the internet. It is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms. parentinfo.org/

Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms. www.parents.parentzone.org.uk/

Appendix 6 Government Guidance and Support / National Organisations for School Staff

National curriculum in England: computing programmes of study - Statutory guidance on computing programmes of study. www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study

Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment. www.gov.uk/government/publications/keeping-children-safe-in-education--2

Behaviour and discipline in schools - Guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour. www.gov.uk/government/publications/behaviour-and-discipline-in-schools

CEOP Thinkuknow Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18, expert and support and professional development for the children's workforce. www.thinkuknow.co.uk/

National Centre for Computing Education (NCCE) has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum. teachcomputing.org/

UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use, published February 2019. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying. www.anti-bullyingalliance.org.uk/

Childnet - a children's charity and has a wide range of practical resources freely available, covering all online safety issues, and which are available for teachers working with children of all ages, including children with SEN. www.childnet.com/

Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety. www.internetmatters.org/schools-esafety/

Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online. www.iwf.org.uk/

NSPCC learning – includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges. learning.nspcc.org.uk/

Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their pupils on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience. parentzone.org.uk/school-zone

UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools. www.saferinternet.org.uk/