Primary
Online Safety Policy

Approved by:	**Governing Body**
Approval Date:	**January 2026**
Review Date:	**January 2028**

Contents

1. Aims

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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, anti-Semitism, radicalisation and extremism, misinformation, disinformation and conspiracy theories.
- **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 scam.

2. Legislation and Guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Governing Board

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

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

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that all staff undergo safeguarding training to include online safety and that this includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Do all that they reasonably can to limit children's exposure potentially harmful and inappropriate online material on the school's IT system.
- Ensure schools have appropriate filtering and monitoring in place and regular review their effectiveness.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the schools' DSL and deputies are set out in our Safeguarding Policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety and understanding the filtering and monitoring systems and procedures in place in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, Trust IT staff and other staff, as necessary, to address any online safety issues or incidents, including reviewing the effectiveness of the school's filtering and monitoring systems.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

- Updating and delivering staff training on online safety ensuring that relevant staff have an awareness and understanding of the provisions in place in regards to filtering and monitoring and that they manage them effectively to know when to escalate concerns identified.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school, including the effectiveness of the filtering and monitoring systems to the headteacher and/or governing board.
- To be responsible for ensuring the standards in the DFE Filtering and Monitoring documentation are met.

3.4 West Norfolk Academy Trust IT Team

The WNAT IT team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the schools' 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 schools' ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Helping to ensure that any online safety incidents are dealt with appropriately in line with this policy.
- Helping to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and anti-bullying policy.

3.5 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 (appendix 3 & 4), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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 and anti-bullying 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'.
- Having an understanding of the expectations, applicable role and responsibilities in relation to filtering and monitoring.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as ClassDojo, and other network resources, safely and appropriately.

3.7 Visitors and Members of the Community

Visitors and members of the community who use the schools' ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

4. Educating Pupils About Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. We have an effective whole school approach to online safety that empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

At our school we ensure online safety is a running and interrelated theme. Pupils will be taught about online safety as part of a broad and balanced curriculum:

- We recognise the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact

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

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.*
- *How information and data is shared and used online.*
- *What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*

The school will use assemblies and other national days to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents About Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

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

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

Parents can seek further guidance on keeping children safe online from a range of organisations and websites, for example:

- https://www.thinkuknow.co.uk/parents/
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childnet.com
- https://www.internetmatters.org

6. Procedures for Responding to Specific Online Incidents or Concerns

6.1 Cyber-Bullying Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy).

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff also find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes lessons using our online safety curriculum (based on dfe Education for a Connected World), computing curriculum (based on NCCE lesson plans), PHSE lessons from Jigsaw and other subjects where appropriate.

All staff, receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Consensual and Non-Consensual Sharing of Nude and Semi-Nude Images and/or Videos (also known as sexting or youth produced sexual imagery);

The school recognises consensual and non-consensual sharing of nudes and semi-nudes and/or videos (also known as youth produced sexual imagery or “sexting”) as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The school will ensure that all members of the community are made aware of the potential consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.

The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

6.4 Dealing with ‘Sexting’

If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will act in accordance with our Child Protection and Safeguarding policies and Behaviour Policies

6.5 Online Child Sexual Abuse and Exploitation

The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.

The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community through the school's website

6.5.1 Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of incident involving online sexual abuse of a child, the school will act in accordance with the school's Child Protection and Safeguarding Policies and Immediately notify the Designated Safeguarding Lead.

- Store any devices involved securely.
- Immediately inform police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.

Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via CEOP

If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the CADS and Norfolk Safeguarding Children Partnership.

If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the CADS by the Designated Safeguarding Lead.

If pupils at other schools are believed to have been targeted, the school will seek support from Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

6.6 Examining Electronic Devices

(This should be read in conjunction with the Trust Staff Code of Conduct: Section 18. Unacceptable Use of ICT Facilities and Monitoring)

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

7.1 Internet Access, Security and Filtering

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

In our schools we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements in the Filtering and Monitoring standards.

7.2 E-mail Our Schools:

- Provide staff with an email account for their professional use (initial.surname@xxxinfant/junior/primary.co.uk) and makes clear personal email should be through a separate account.
- We use anonymous e-mail addresses, for example head@, office@
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.

7.3 Pupils Email:

- We use school provisioned pupil email accounts that can be audited
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.
- Pupils will sign an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.4 Staff Email:

- Staff will use Trust or school provisioned e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Staff will not use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

7.5 School Websites

- The schools web sites comply with statutory DfE requirements.
- Most material is the schools' own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- The school will post information about safeguarding, including online safety, on the website;
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. (See Staff Code of Conduct Section 17).

7.6 Management Information System Access and Data Transfer

- Teachers and office staff have access to the MIS (Bromcom).
- Data on this system must not be copied or shared with any other person and kept confidential.
- Staff must log out of the MIS when they are not near the computer.

7.7 Social Networking - Staff, Volunteers and Contractors

- The use of any school approved social networking (e.g School Twitter Account or School Facebook account) will adhere to ICT Acceptable Use Agreement
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Executive Headteacher.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

7.8 Digital Images and Video

In our schools:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the schools' Acceptable Use Agreement and this includes a clause on the use of personal mobile phones/personal equipment

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our *[age appropriate]* pupil Acceptable Use Policy (Appendix 1 & 2)

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our Acceptable Use Policy and additional communications materials when required.

Communicating with Pupils, Parents and Carers

- School will communicate with parents via approved official channels eg school website, email, Class Dojo, school Twitter account etc. All communication will comply with the Trust Data Protection Policy and Privacy Notices.

8. Bring Your Own Device Guidance for Staff and Pupils

- Personal devices *(smartphones, laptops, personal tablets etc.)* should not be connected to the schools' wifi.
- Pictures of children should not be taken on personal devices.
- Personal devices, other than smartphones, are discouraged from being brought into school.

Pupils Using Mobile Devices in School

- Only in certain circumstances, with express permission of the Headteacher, may some pupils bring a mobile device into school. Mobile phones must be handed into the school office during the day, and pupils' may collect them at the end of the day but are not permitted to use them during the school day.
- Any use of mobile devices in school by pupils must be in line with the acceptable use policy.
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff Using Work Devices Outside School

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- If staff have any concerns over the security of their device, they must seek advice from the Trust ICT technician
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.

10. How the Schools will Respond to Issues of Misuse (Also see Staff Code of Conduct)

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures, in line with current guidance from the Department for Education, as set out in our policies on Behaviour, and Internet Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The DSL acts as the first point of contact for any safeguarding incident whether involving technologies or not. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with by the Headteacher, in accordance with the Staff Disciplinary Procedures and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

In our schools:

- There is strict monitoring and application of the Online Safety Policy, including the ICT Acceptable Use Policy and a differentiated and appropriate range of sanctions.
- Support is actively sought from other agencies as needed *(i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police)* in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within our schools.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- We will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the Trust.
- For any breach of the acceptable use policy, the school will follow the agreed sanctions described in appendix 5 of this policy.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including filtering and monitoring, cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

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

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

safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every annually by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board.

13. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy
- AI policy

Appendix 1

Pupil Acceptable Use Policy

Safe

- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are appropriate and if I have permission.
- I only talk with and open messages from people I know, and I only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, image or text I use.

Responsible

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school computers for school work, unless I have permission otherwise.
- I know that personal devices are not permitted in school.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.
- I will only change the settings on the computer if a teacher/technician has allowed me to.

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules then I will receive a sanction.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page, shut the lid and tell an adult straight away.

We request that children at our school sign and return the agreement form to ensure that we respect the rules around online safety. This is a safeguarding matter which will benefit everyone.

Pupil Acceptable Use Policy Form

Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the pupil Acceptable Use Policy (AUP).

I agree to follow the pupil AUP when:

1. I use school systems and devices, both on and offsite.
2. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website.

Pupil name……. Signed…….

Class…… Date…….

Parents Name…….....

Parents Signature……. …….

Date…….

Appendix 2

Parent/Carers Acceptable Use Policy

1. I have read and discussed the School Acceptable Use Policy with my child.
2. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence, then the Police will be contacted.
7. I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community. I will not share other pupils work from Class Dojo.
8. I know that I can speak to the school Designated Safeguarding Lead Louise Jackson, my child's teacher or the headteacher if I have any concerns about online safety.
9. I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:

    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com

11. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I have read, understood and agree to comply with the School Acceptable Use Policy.

Child's Name…… Class……

Parents Name……

Parents Signature……

Date……

Appendix 3

Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR). o This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. o Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected. This may include data being encrypted by a method approved by the school.

- **Emails used for school business must be official work emails and not personal emails**
- Any images or videos of pupils will only be used for school business and will always reflect parental consent.

7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school google drive to upload any work documents and files

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media and the supervision of pupils within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Trust ICT Team as soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

    - All communication will take place via school approved communication channels, such as a school provided email address, Class Dojo or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones. o Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.

    - I will take appropriate steps to protect myself online as outlined in the Online Safety Policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the Trust Code of Conduct/Behaviour Policy and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Headteacher.

18. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

20. I understand my role and responsibilities in relation to filtering and monitoring and understand the provisions that are in place to manage them effectively and know how to escalate concerns when identified.

I have read, understood and agreed to comply with the School Staff Acceptable Use Policy.

Name ……..

Signed…….

Date:……

Appendix 4

Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.

- I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

- All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.

- Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Headteacher.

- My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or

anything which could bring my professional role, the school, or the County Council, into disrepute.

- I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead or the Headteacher.

- I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

- I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the School's Visitor / Volunteer Acceptable Use Policy.

Name:…… Signed:…….

Date:……..

Appendix 5

Sanctions for Unacceptable Use

- Parents will be informed immediately
- A temporary or permanent ban from Internet access
- A temporary or permanent ban from the use of school's ICT facilities
- Access to the Internet may be withdrawn.
- A serious breach of the policy will result in further disciplinary action being taken, including suspension or expulsion.
- If it is suspected that a criminal offence has been committed the appropriate authorities will be informed
- Appropriate additional disciplinary action if the action breaks any other school rule or convention.
- This action will be defined in the Whole School Behaviour Policy and/or Anti-bullying Policy – Cyberbullying Policy
- Where applicable, referral to appropriate external agencies.