



Windmill Primary Federation Online Safety Policy

Approved by: Governing Body

Approval Date: October 2025

Review Date: October 2026

Contents

1. Aims	3
2. Legislation and Guidance	3
3. Roles and Responsibilities	4-6
4. Educating pupils about online safety	6-7
5. Education parents about online safety	7-8
6. Procedures for specific online concerns	8-10
7. Acceptable use of the internet for school	11-13
8. Pupils using mobile devices in school	13
9. Staff using work devices outside school	13
10. How the schools will respond to issues of misuse (Also see Staff Code of Conduct)	14
11. Training	14-15
12. Monitoring Arrangements	15
13. Links with other policies	15
Appendix 1: Pupil Acceptable Use Agreement	16-17
Appendix 2: Staff Acceptable Use Agreement	18-23
Appendix 3: Sanctions for Unacceptable Use	23

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.
- **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, 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 ICT Service

The Rydall 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.

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.
- 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.
- **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 e-safety curriculum (based on dfe Education for a Connected World), computing curriculum (based on NCCE lesson plans), PHSE lessons 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 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 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 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 (initialsurname@windmillfederation.org.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 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;

7.6 Management Information System Access and Data Transfer

- Teachers and office staff have access to the MIS (Pupil Asset).
- 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, Seesaw, etc. All communication will comply with the Federation 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 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 Headteacher.
- 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

;|;

Appendix 1 - Pupil Acceptable Use Policy

Key Stage 1

- I only use the internet at school when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information safe.
- I will not share my passwords with anyone.
- I only send messages online which are polite and friendly.
- I know the school/setting can see what I am doing online.
- I know I am not allowed my personal devices in school
- I always tell an adult/teacher/member of staff if something online makes me feel unhappy or worried.
- I know what might happen to me at school if I do not follow the rules:
 - My parents will be told
 - I will receive a sanction
 - If it is serious, the Police may be informed
 - I have read and talked about these rules with my parents/carers

Agreement

I am signing below to show that I have discussed this with my child and they understand that they must try to abide by these rules.

Pupils Name	
Parent/Carer Signature	
Date	

Key Stage 2

Acceptable Use Policy / Agreement

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carers.
- I will only open email attachments if it has been approved by a member of school

staff in school or a parent/carer out of school. If I am unsure about an attachment, I will ask an adult for help.

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

- Speak to me about my behaviour
- Speak to my parents/carers about my use of technology
- Remove me from online communities or groups
- Not allow me to use laptops/computers or other mobile devices to access the internet, school computer network or particular programmes and apps.
- Take any other action necessary to keep me and others safe.

Agreement

I am signing below to show that I understand and will try to abide by these rules

Pupils Name	
Parent/Carer Signature	
Date	

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 - 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.

Staff E-Safety and Acceptable Use Policy / Agreement

All staff should read and sign this document and agree with the statements.

This policy covers the following aspects of e-safety in relation to all school staff:

- Use of school-based equipment
- Social Networking
- Managing digital content
- Email
- Mobile phones and devices
- Learning and teaching

School Policy

Modern technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use policy agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people. I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data out of school.

Use of school-based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements.

- I will access the internet and other ICT systems using my personal username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the e-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher/ DSL.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- 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, I will report this to Rydall.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g., by an open window or on the back seat of a car.
- Wherever possible I will use school provided cloud storage solutions to move files between devices. If I have to use a portable storage device (USB sticks, SSD cards, portable hard drives etc) I will ensure that it has been approved for use on the school network by the Head of School/ Executive Headteacher
- I will ensure that any personal or sensitive information taken off site will be stored on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create or have access to from other information systems, which could be deemed as personal or sensitive will be either stored on the school network or school provided cloud storage and access controlled in a suitable manner in accordance with the school data protection controls. (For example,

spread sheets/other documents created from information located within the school information management system).

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the Head of School/ Executive Headteacher
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and computer activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- I know that staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to a DSL

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school or for school use.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy/ Home School Agreement (or any other relevant policy).
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the device memory.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to

this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will use my school email address for all email correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- Any personal device used to access school email or other communication systems will be encrypted and secured using a password in line with the school's password policy or biometric technology.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I will comply with the privacy requirements of GDPR and the 2019 DPA when sending emails to groups of people by ensuring that all such emails are sent to Undisclosed Recipients.
- Emails sent to external organisations will be written carefully and if necessary, authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account and delete emails no longer required. Information I have a legitimate need to retain will not be kept in my email inbox but will be saved appropriately in the school's chosen storage system, ensuring access for other users if appropriate.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances. If I have to keep Bluetooth turned on, I will ensure that the connection has a name appropriate to the setting.
- I will not contact any parents or pupils on my personally owned device.
- I will not use any personally owned mobile device to take images, video or sound recordings.

Learning and teaching

- In line with every child's legal entitlement, I will ensure I teach an age and stage appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe

and responsible behaviour in pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources and the use of AI generated content at all times.

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name	
Role in School	
Signed	
Date	
Accepted by	
Date	

Appendix 3 - 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.