WITTERING PRIMARY SCHOOL

E-Safety Policy

Date Of Agreement: **May 2023**

Signed:

Proposed Review Date : May 2025

Rationale

Our E-Safety Policy has been written by the school, building on local and government guidance. It has been agreed by the staff and approved by the governors.

This policy applies to all school related activity by the school community and takes effect throughout all other policies within school.

Core Principles Of Internet Safety

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks to pupils, staff, volunteers and governors. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements while delivering an effective approach to online safety. The policy established clear mechanisms to identify, intervene and escalate an incident, where appropriate.
The Headteacher and Deputy Head or, in their absence, the authorised member of staff for e-safety (E-Safety subject leader) and the Computing Co-ordinator has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

There will be a core e-safety group comprising of the Headteacher, Deputy Headteacher, E-Safety Co-ordinator, Computing Co-ordinator and the nominated e-safety governor.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 2021 (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.

The policy also takes into account the National Curriculum computing programmes of study and the Teach computing programme of Study.

Roles and Responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation. The governing body 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).

The governor who oversees online safety is Mrs J. Hunt

All governors will:

Ensure that they have read and understood this policy
Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The head teacher and E-Safety Co-ordinator

The head teacher and E-Safety Co-ordinator are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL's) are set out in our child protection and safeguarding policy.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with IT providers and school staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with school 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the governing body.

This list is not intended to be exhaustive.

The IT provider

The IT provider, St Johns Church School are 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 school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL or DDSL's to ensure that any online safety incidents are logged and dealt with appropriately in line with school policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the head teacher 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 (appendix 1)
-

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's 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 2).

Teaching and Leaning

Why internet use is important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

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

Internet use will enhance learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

The school will try to ensure that the use of internet-derived materials by staff and pupils complies with copyright law.

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

Educating pupils about online safety

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

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

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

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

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly. The ICT provider, St Johns Church School, will ensure virus protection is updated on laptops.

E-Mail

Pupils will have access to email on their Google accounts. The teacher is responsible for managing how these are used within the classroom setting.

Pupils must immediately tell a teacher if they receive offensive e-mail.

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

The forwarding of chain letters is not permitted.

E-mail sent by staff from school based accounts should include the following text:

The content of this e-mail communication (including attachments) is strictly confidential and is intended solely for the use of the named recipient(s). If you have received this e-mail in error, you are not permitted to disclose, distribute, retain or take any action in reliance thereon and are requested to please notify the sender immediately by return e-mail and then delete it.

Wittering Primary School is neither liable for the proper, complete transmission of the information contained in this communication, nor any delay in its receipt. Wittering Primary School does not guarantee that the mail is virus-free. It is the responsibility of the named recipient(s) to check that incoming e-mails are virus free. Wittering Primary School is not liable whatsoever for loss or damage resulting from the opening of this message and/or attachments and/or the use of the information contained in this message and/or attachments.

The views and opinions expressed in this E-mail are those of the sender and no liability will attach to Wittering Primary School. Wittering Primary School retains the copyright to all e-mail messages sent from its communications systems. This e-mail disclaimer will at all times take precedence over any other e-mail disclaimer received by employees / students utilising the communications facilities of the school.

Published content and the school web-site

The contact details on the web-site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Pupils' full names will not be used anywhere on the web-site or any blogs, particularly in association with photographs.

Pupils' work or photos can only be published with the permission of the parents.

Social networking and personal publishing

Updata (or the network provider), at the schools request, will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

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

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Staff may use social media accounts for educational purposes under the direction of the headteacher. During this use, no photographs of children or personal information is to be shared.

Managing filtering

The school will work with Updata and other IT partners to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Subject Leader, or in their absence the Headteacher or Deputy Headteacher.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Managing videoconferencing

Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

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

Other devices

Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.

The sending of abusive, offensive or inappropriate material is forbidden.

Games machines including the Sony PlayStation, Microsoft Xbox, Nintendo Wii, Nintendo Switch and others have Internet access which may not include filtering. Care will be taken if they are used within the school.

Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Cyber-bullying

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.) Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

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 follow procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service
- The provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying or behaviour policy.
- Parent and carers of pupils will be informed.
- The police will be contacted if a criminal offence is suspected.

Technical Infrastructure

Policy Decisions

Authorising internet access

The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date.

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

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Updata can accept liability for the material accessed, or any consequences of internet access.

The school and/or its IT partners will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

If a genuine mistake is made such, as inappropriate results from a google search appear, then the Headteacher should be informed (E-Safety Co-ordinator and Deputy Head in their absence) so that the incident can be recorded.

All adults within school will be actively aware of signs for extremism and how it may arise during internet usage. Any concerns are to be directly referred to the headteacher.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by the headteacher (in a case of misuse by the headteacher the case will be dealt with by the chair of governors.)

Any complaint about misuse must be referred to the headteacher using My Concern.

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

Pupils and parents will be informed of the complaints procedure.

Communications Policy

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 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 2 and 3

Introducing the E-Safety Policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and internet use will be monitored.

E-safety lessons will be part of the computing curriculum.

Staff and the E-Safety Policy

All staff will be given access to the School E-Safety Policy and its importance explained.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure, have Bitlocker enabled and be password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT support, St Johns Church School.

Work devices must be used solely for work activities.

Enlisting parents' support

Parents' attention will be drawn to the school's E-Safety Policy in newsletters and on the school web-site.

Pupils and parents will be informed of consequences for pupils misusing the Internet.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher/DSL or any of the DDSL's

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

Community use of the Internet

All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 in accordance with the staff disciplinary procedures and code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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

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, e-bulletins and staff meetings).

The DSL and DDSL's 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 safeguarding and child protection policy.

Monitoring arrangements

The DSL and/or DDSL's log behaviour and safeguarding issues related to online safety. Reports must be completed on My Concern, as referenced in the school Child Protection and Safeguarding Policy.

This policy will be reviewed every three years by the E-Safety Co-ordinator. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy
Behaviour policy
Staff disciplinary procedures
Staff code of conduct policy
Data protection policy and privacy notices
Complaints procedure

Signed ……. (Chair of Governors) Date ……..

To be reviewed September 2025

Appendix 1: acceptable use agreement for pupils and parents/carers

Acceptable use of Wittering Primary School's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of Wittering Primary School's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and/or deputy designated safeguarding leads (DDSL) aware if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Wittering Primary School's online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	