



Intack Primary School: Online Safety Policy

Policy Status: Agreed by Governors 30th June 2026

Date of Creation: 9th October 2025

Date of Review: June 2026

Reviewer: Headteacher and Governors' Committee

Next Review Date: October 2026

Contents

1. Aims	2
2. Legislation and guidance.....	2
3. Roles and responsibilities.....	2
4. Educating pupils about online safety	4
5. Educating parents about online safety	5
6. Cyber-bullying	5
7. Acceptable use of the internet in school.....	6
8. Pupils using mobile devices in school	6
9. Staff using work devices outside school.....	7
10. How the school will respond to issues of misuse	7
11. Training	7
12. Monitoring arrangements	8
13. Links with other policies	8
Appendix 1: Acceptable use agreement (pupils and parents/carers)	9
Appendix 2: Acceptable use agreement (staff, governors, visitors and volunteers)	11
Appendix 3: online safety training needs – self audit for staff	13
Appendix 4: online safety incident report log	14

1. Aims

Our school aims 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, including mobile and smart technology (which we refer to as 'mobile phones')
- › 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 DfE'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.

The policy also takes into account the National Curriculum computing programmes of study.

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).

The governor who oversees online safety is [Mr Abdul Qadoos](#).

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 (appendices)

- › 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 school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- › Managing all online safety issues and incidents in line with the school child protection policy
- › Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- › Liaising with other agencies and/or external services if necessary
- › Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager (Blue Orange)

The ICT manager is responsible for:

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

This list is not intended to be exhaustive.

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 and ensuring that pupils follow the school's terms on acceptable use (see appendices)

- › Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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'

This list is not intended to be exhaustive.

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)

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

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)
- › Healthy relationships – [Disrespect Nobody](#)

3.7 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 (appendices).

4. Educating pupils about online safety

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

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- › [Relationships education and health education](#) in primary schools
- › [Relationships and sex education and health education](#) in secondary schools

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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 or Facebook page. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with any member of staff in school.

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

6. Cyber-bullying

6.1 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. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 Examining electronic devices

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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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). 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 the appendices.

8. Mobile devices in school

At Intack Primary School:

- Mobile phones including smart watches are not allowed in school. Parents are asked to speak to the Headteacher for any specific reasons a child may need to have one with them.
- Any mobile phones agreed by the Headteacher will need to be handed in as the child enters school. This will be kept secure in the Headteacher's room and returned at the end of the day, or when the pupil leaves the building.
- Phones are to be switched off until they are returned to the child at the end of the day
- We will teach pupils the risks that are associated with the use of mobile phones, both in school and more broadly, to ensure they understand the decision being taken by their school to prohibit the use of mobile phones throughout the school day

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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Not to be used in the presence of children at any time.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the appendices.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the School Business Manager.

10. 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 our policies on behaviour and ICT and internet acceptable use. 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/staff 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.

11. 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content, physical abuse, sexual violence and initiation/hazing type violence can all contain an online element



Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and 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. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the SLT (including the headteacher) and the FGB. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy



Appendix 1: Acceptable use of the internet agreement

The Intack Acceptable Use Agreement

This agreement explains how parents and carers can help support safe and responsible use of technology at Intack Primary School. We want to work in partnership with families to ensure all children use technology confidently, respectfully, and safely, both in school and at home.

Our Promise:

At Intack Primary School, we use computers, tablets, and the internet to help us learn, create, and share. We promise to use technology safely, kindly, and responsibly at school and at home.

Supporting Safe and Responsible Technology Use

As a parent/carers, I agree to:

- Support my child in following the school's Pupil Acceptable Use Agreement.
- Supervise my child's online activity at home and ensure they only use age-appropriate games, websites, and apps.
- Support the school's approach to online safety and digital learning.

1. Being Safe Online

My child will:

- Keep personal information (like full name, address, or passwords) private.
- Tell an adult if they see or hear something online that worries or upsets them.
- Only use websites, games, or apps that an adult has said are OK.
- Ask a teacher or parent before downloading or clicking on something new.

2. Being Kind and Respectful

My child will:

- Use kind words when online or sending messages.
- Respect other people's work, pictures, and ideas.
- Never post or share pictures or videos of anyone without permission.
- Remember that what they do online should make our school a happy and safe place.

3. Using Technology for Learning

My child will:

- Use school devices for learning, not for games or chatting unless a teacher says it's okay.
- Take care of school equipment and use it responsibly.
- Log out when finished and keep passwords secret.
- Ask for help if they are not sure what to do.

4. Using AI Safely

My child will:

- Use AI tools (like ChatGPT or other learning apps) safely and responsibly.
- Ask a teacher or parent if unsure about what to type or share with AI.
- Remember that AI can make mistakes, so they will check important answers or information.
- Never share personal information, passwords, or anything private with AI.
- Use AI to help learn and create, not to cheat or be unkind.

Communication and Online Conduct

As a parent/carers, I agree to:

- Use school communication tools (such as email and Purple Mash) for educational purposes only.
- Communicate with staff respectfully and courteously.



- Never share or discuss confidential or sensitive school matters, pupils, or staff on social media.
- Avoid posting or sharing photos or videos that include other pupils or staff without their consent.
- Contact the school directly with any concerns instead of posting online.

5. Working Together

My child understands that:

- Teachers and adults at school can check what they do on school computers and the internet.
- If they break these rules, they might lose their computer or internet privileges for a while.
- These rules help keep everyone safe and happy.

Privacy, Data, and Monitoring

As a parent/carer, I agree to:

- The school using filters and monitoring tools to help protect pupils while online.
- Staff reviewing technology use to ensure it remains safe and appropriate.
- The school handling personal information in line with its Privacy Notice and data protection laws.
- Any online learning tools used by the school have been checked for safety and data compliance

6. Signatures

By signing this, we agree to follow the rules for using technology safely and responsibly, at school and at home.

Child's Name: _____ Parent / Carer Name: _____

Child's Signature: _____ Parent / Carer Signature: _____

Class: _____ Date: _____



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

Staff Acceptable Use Agreement

This agreement sets out expectations for all staff, volunteers and contractors who work with our pupils, use technology, digital systems, or online communication on behalf of Intack Primary School.

Its purpose is to protect staff, pupils and the school by promoting safe, professional and responsible use of digital technology.

1. Professional Use of Technology

As a member of staff, I agree to:

- Use school technology and online systems primarily for educational or professional purposes.
- Keep personal and professional data separate.
- Protect passwords and logins and never share them with pupils or colleagues.
- Lock or log off devices when not in use.
- Report any technical or security concerns (e.g. data breaches, suspicious emails) to the Designated Safeguarding Lead (DSL), Blue Orange or the IT lead immediately.
- Avoid using personal devices to store or share pupil data unless specifically authorised and compliant with school policy.

2. Communication and Conduct

I agree to:

- Communicate with pupils, parents and colleagues in a professional and respectful manner at all times.
- Only use approved school communication channels (e.g. official email, school apps, VLP, etc.).
- Never use personal email, phone, messaging, or social media accounts to contact pupils or parents.
- Use social media responsibly and ensure posts or comments do not bring the school, colleagues, or pupils into disrepute.
- Avoid posting identifiable school content, images or pupil information on personal accounts.

3. Data Protection and

Confidentiality I understand that:

- I must follow the school's **Data Protection Policy, Online Safety Policy, Acceptable Use Policy** and **Privacy Notice** at all times.
- Personal data must be handled securely and in accordance with GDPR.
- Sensitive or confidential information (including photos or documents containing personal data) must not be shared via unsecured platforms.
- Any data loss or breach must be reported immediately.

4. Safe Use of AI (Artificial Intelligence) I agree to:

- Use AI tools (e.g. ChatGPT, Microsoft Copilot, AI-based learning or marking tools) responsibly, for educational or administrative support only.
- Check the accuracy and appropriateness of AI-generated content before using or sharing it.
- Avoid inputting any personal, confidential, or pupil-identifying information into AI systems.
- Model responsible AI use for pupils, reinforcing safe, critical and ethical use of technology.

5. Use of Images, Video, and Recordings I agree that:

- I will only capture, store or share images or videos of pupils when there is a clear educational or school purpose and appropriate consent has been obtained.
- I will only use school-owned or approved devices for capturing or storing such content.
- I will ensure that all images and videos are stored securely and deleted when no longer needed.
- I will not share photos or videos of pupils on personal social media accounts under any circumstances.

6. Personal and Professional Boundaries I understand that:

- I must maintain appropriate professional boundaries with all pupils, in person and online.
- I must not engage in one-to-one online communication with pupils outside of approved school platforms.
- Any concerns about staff or pupil online behaviour must be reported to the Designated Safeguarding Lead.

7. Agreement and Declaration

By signing this document, I confirm that:

- I have read and understood this Acceptable Use Agreement.
- I will follow the school's policies on safeguarding, data protection, online safety and ICT use.
- I understand that any breach of this agreement may result in disciplinary action and/or withdrawal of access to school systems.

Staff Name: _____

Signature: _____

Position/Role: _____

Date: _____

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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?	



Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident