# IGHTENHILL PRIMARY SCHOOL

# Online Safety Policy 2026 - 2027

| | | |
|---|---|---|
| Approved by: | The Governing Body | Date: November 2026 |
| Last reviewed on: | November 2026 | |
| Next review due by: | November 2027 | |

## Contents

1. Aims ..... 2
2. Legislation and guidance ..... 3
3. Roles and responsibilities ..... 3
4. Educating pupils about online safety ..... 5
5. Educating parents about online safety ..... 6
6. Cyber-bullying ..... 7
7. Acceptable use of the internet in school ..... 8
8. Pupils using mobile devices in school ..... 8
9. Staff using work devices outside school ..... 8
10. How the school will respond to issues of misuse ..... 9
11. Training ..... 9
12. Monitoring arrangements ..... 10
13. Links with other policies ..... 10
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) ..... 11
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) ..... 12
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) ..... 13
Appendix 4: online safety training needs – self audit for staff ..... 14
Appendix 5: online safety incident report log ..... 15

## 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 Mrs Lewis and Mr Atherton

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, 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 E Brown [and deputies S Crosier and K Dunderdale] 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 (Apex) 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 5) 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 4 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 Computing subject leader (working with our IT support company)

The Computing leader (working with our ICT support company (Apex Network Solutions) 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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.

## 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), 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 (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of child-on-child abuse are dealt with appropriately in line with the school behaviour policy. This can happen within cyber-bullying which can include, but is not limited to: consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery; upskirting which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals of buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

All staff should be aware that children can abuse other children (often referred to as child on child abuse) and that it can happen both inside and outside of school or college and online It is important that all staff recognise the indicators and signs of child on child abuse and know how to identify it and respond to reports.

- All staff should understand, that even if there are no reports in their school, it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have any concerns regarding child on child abuse they should speak to their designated safeguarding lead (or deputy).
- 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 (appendix 3).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The children will be taught online safety lessons each half term. The children at Ightenhill also review our Children's Online Safety Policy at the start of each academic year.

The text below is taken from the National Curriculum computing programmes of study.

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 remote learning platform (Class Dojo). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings. Parents are invited in during Safer Internet Day to discuss online safety and to ask any questions.

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.

# 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 pupils.

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
- The school's COVID-19 risk assessment

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.

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 1, 2 and 3.

## 8. Use of mobile devices in school

Please refer to our use of mobile devices in school policy.

## 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

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 Computing subject leader or the Headteacher.

## 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 ICT and internet acceptable use agreements. 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 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 back-up DSL 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 Headteacher and Computing Subject Leader.

At every review, the policy will be shared with the governing board. The review (such as the one available here) 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 Management policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement
- GDPR policies (data protection policy, data breach procedure, pupil privacy notice, workforce privacy notice, subject access procedures, retention schedule and parent privacy notice)
- Children's Online Safety Policy (Appendix 6).

## Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| Name of pupil: | |
| When I use the school's ICT systems (like computers) and get onto the internet in school I will:<br>• Ask a teacher or adult if I can do so before using them<br>• Only use websites that a teacher or adult has told me or allowed me to use<br>• Tell my teacher immediately if:<br>  ○ I click on a website by mistake<br>  ○ I receive messages from people I don't know<br>  ○ I find anything that may upset or harm me or my friends<br>• Use school computers for school work only<br>• Be kind to others and not upset or be rude to them<br>• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly<br>• Only use the username and password I have been given<br>• Try my hardest to remember my username and password<br>• Never share my password with anyone, including my friends.<br>• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer<br>• Save my work on the school network<br>• Check with my teacher before I print anything<br>• Log off or shut down a computer when I have finished using it<br>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules. | |
| 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 will make sure my child understands these. | |
| Signed (parent/carer): | Date: |

## Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| Name of pupil: | |
| I will read and follow the rules in the acceptable use agreement policy<br>When I use the school's ICT systems (like computers) and get onto the internet in school I will:<br>• Always use the school's ICT systems and the internet responsibly and for educational purposes only<br>• Only use them when a teacher is present, or with a teacher's permission<br>• Keep my username and passwords safe and not share these with others<br>• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer<br>• Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others<br>• Always log off or shut down a computer when I'm finished working on it<br>I will not:<br>• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity<br>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>• Use any inappropriate language when communicating online, including in emails<br>• Log in to the school's network using someone else's details<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision<br>If I bring a personal mobile phone or other personal electronic device into school:<br>• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission<br>• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online<br>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules. | |
| Signed (pupil): | Date: |
| Parent/carer's 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 3: acceptable use agreement (staff, governors, volunteers and visitors)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND 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 (if applicable), I will not:<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>• Use them in any way which could harm the school's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share my password with others or log in to the school's network using someone else's details<br>• Take photographs of pupils without checking with teachers first<br>• Share confidential information about the school, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the school | |
| 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.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I will let the designated safeguarding lead (DSL) and ICT manager know 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.<br>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 4: 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 5: 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 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Appendix 6: Children's Online Safety Policy

What is online safety about?

At Ightenhill Primary School, we want to help you and teach you how to stay safe online.

There are four areas of online safety that we will learn about called the 4 C's.

| | |
|---|---|
| **Content**<br>This area is all about what you post online and what you look at online. Is it appropriate for your age? | **Contact**<br>This is all about who you are speaking to online. Do you know them? |
| **Conduct**<br>This area is all about how you act online and how other people act towards you. Are they being kind? | **Commerce**<br>This area is about being tricked online to either buying things, gambling or tricks websites use to get your money. |

If you are worried about something that is happening to you online, you can:




Staying safe online at school

- Keep your passwords and usernames private.
- Use an avatar rather than a picture of yourself
- Only google appropriate things. We monitor everything that happens online. Be responsible.
- Look after our school equipment. Treat it with respect.

If something appears on your device that you don't think you should see, tell your teacher so that they can help you.

Class: _____ (children to sign the back of the sheet)

Date: _____