



# Online Safety Policy - January 2026

## Honeywell Ethos Statement

*"A community that cares about excellence, wonder and learning for life"*

*We provide a safe and exciting space where:*

### *There is community*

- There is a strong, friendly and respectful spirit within the immediate and extended communities, supporting learning and progress of and for all pupils*
- There is a sense of belonging*

### *There is care*

- 1. Everyone focusses on valuing and developing the whole child, nurturing a happy and kind atmosphere where asking for help and listening is what we expect of each other*
- 2. We understand our actions and nurture respect for each other and the environment*

### *There is excellence*

- 3. There is a strong sense of ambition and high academic achievement along with excellent personal progress built around quality first teaching and research informed learning,*
- 4. There is enrichment and high expectations beyond the curriculum*

### *There is wonder*

- 5. Every experience is more memorable than the last*
- 6. Learning powers are nurtured and grow and grow*
- 7. The implementation of the curriculum is rich, vibrant and creative*

### *There is learning for life*

- 8. There is an unstinting dedication to diversity and equality*
- 9. There is motivation for the preservation of our environment and a thirst to become a conscientious contributor to making the world a better place*
- 10. Pupils leave us with a thirst for knowledge and love of learning, autonomous and self-motivated, ready for their next stage and beyond*

## Contents

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| Aims .....                                                                                  | 2  |
| Legislation and Guidance .....                                                              | 2  |
| Links With Other Policies .....                                                             | 2  |
| Roles and Responsibilities.....                                                             | 2  |
| Educating Pupils About Online Safety.....                                                   | 4  |
| Educating Parents/Carers About Online Safety .....                                          | 5  |
| Cyber-Bullying .....                                                                        | 5  |
| Acceptable Use of The Internet in Schools .....                                             | 6  |
| Filtering and Monitoring .....                                                              | 7  |
| Staff Using Personal Devices Inside School.....                                             | 7  |
| Staff Using Work Devices Outside School .....                                               | 7  |
| How the Schools Will Respond to Issues of Misuse .....                                      | 7  |
| Training .....                                                                              | 8  |
| Monitoring Arrangements .....                                                               | 8  |
| Appendix 1: Digital 5 A Day.....                                                            | 9  |
| Appendix 2: EYFS And KS1 Acceptable Use Agreement.....                                      | 10 |
| Appendix 2: KS2 Acceptable Use Agreement.....                                               | 11 |
| Appendix 3: Acceptable Behaviours and Use Agreement (Staff, Governors and Volunteers) ..... | 13 |
| Appendix 4: Acceptable Behaviours and Use Agreement (Parents and Carers).....               | 15 |
| Appendix 5: Acceptable Use Agreement (Visitors and Contractors ) .....                      | 17 |
| Appendix 6: Example Online Safety Incident Report Log.....                                  | 18 |
| Appendix 7: Example ONLINE SAFETY TRAINING NEEDS AUDIT .....                                | 19 |

## Aims

Our schools aim to:

-  Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
-  Identify and support groups of pupils that are potentially at greater risk of harm online than others
-  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 and smart watches')
-  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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, 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 the user 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 scams

## Legislation and Guidance

This policy is based on the Department for Education's (DfE's) 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 Head Teachers and school staff](#)
-  [Relationships and sex education \(RSE\) and health education](#)
-  [Searching, screening and confiscation](#)
-  DfE's guidance on [protecting children from radicalisation](#).
-  [Education Act 1996](#) (as amended)
-  [Education and Inspections Act 2006](#)
-  [Equality Act 2010](#).
-  [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.

## Links With Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policies
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT And Internet Acceptable Use Policy

## Roles and Responsibilities

**The Governing Body, led by Online Safety and Safeguarding Link Governor:**

-  Has overall responsibility for monitoring this policy and holding the Head Teachers to account for its implementation.
-  Will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
-  Will make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

-  Will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
-  Will make sure that the schools teach pupils how to keep themselves and others safe, including online.
-  Will make sure that the schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness
-  Will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers, in conjunction with the DSL, what needs to be done to support the school in meeting the standards, which include:
  - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
  - Reviewing filtering and monitoring provisions at least annually
  - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
  - Having effective monitoring strategies in place that meet the schools' safeguarding needs

#### **All Governors will:**

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the schools' approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND) 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

#### **The Head Teachers are:**

- Responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the schools.

#### **The Designated Safeguarding Leads (DSLs)**

Details of the schools' designated safeguarding leads (DSLs) [and deputies] are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions. The DSLs takes lead responsibility for online safety in school, in particular:

- Supporting the Head Teachers in making sure that staff understand this policy and that it is being implemented consistently throughout the schools
- Working with the Head Teachers and Governing Body to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing Governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT Manager to make sure the appropriate systems and processes are in place
- Working with the Head Teachers, 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 schools' Child Protection Policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- Making sure 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 7 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 both schools to the Head Teachers and/or Governing Body
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

#### **The ICT manager – Currently Wavenet**

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess

effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Making sure 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- Making sure 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**

Staff and volunteers relates to all permanent staff, agency staff, governors, contractors (e.g. club providers), staff engaged from outside agencies to work directly with pupils and all 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 schools' ICT systems and the internet (appendix 3), and making sure that pupils follow the schools' terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by immediately alerting the School Business Manager and Head Teachers
- Following the correct procedures by getting permission from the Head Teachers if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with each school's 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.

#### **Parents/Carers**

Parents/carers are expected to:

- Agree to and sign the Acceptable Behaviours and Use Agreement in Appendix 4.
- Notify a member of staff or the Head Teachers of any concerns or queries regarding this policy
- Make sure that 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- Parents can seek additional information via the following resources:
  - What are the issues? – [UK Safer Internet Centre](#)
  - Help and advice for parents/carers – [Childnet](#) Parents and carers resource sheet – [Childnet](#)

#### **Visitors**

Visitors who use the schools' ICT systems or internet will be supervised by a member of staff and made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 5).

### **Educating Pupils About Online Safety**

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

The text below is taken from the [National Curriculum computing programmes of study](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for introduction 1 September 2026\)](#). All schools have to teach:

- [Relationships education and health education](#)

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

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, for example the AUP available using symbols.

### **Educating Parents/Carers About Online Safety**

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

The school will let parents/carers know:

- What systems the schools use to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the schools (if anyone) their child will be interacting with online

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

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

### **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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

#### **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 encourage them to do so, including where they are a witness rather than the victim. The schools 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 classes. This will also be covered by SLT in assemblies.

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 and citizenship (PSHCE) 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 schools also send information/leaflets on cyber-bullying to parents/carers so 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 each schools' behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the schools will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### Examining Electronic Devices

Neither school allows mobile phones or smart watches. In the Infant school if a child is found to have a phone, the teacher will keep it and return it to the parent or carer at the end of the day. In the Junior school every classroom has a mini safe and children are expected to hand in their phone at the beginning of the day and it is returned at the end of the day. Members of the Senior Leadership Team will take a phone and hand it to the appropriate teacher if a child is found to have it out in the playground prior to 9.00am.

Any member of staff authorised to do so by the Head Teachers can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting a child is in possession of a device during the school day that they say they do not have or if there has been an allegation regarding the content on a phone. Before a search the member of staff will seek the pupil's co-operation. Authorised staff members may examine the content and if inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Head Teachers / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- The DfE's latest guidance on [searching, screening 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 inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

### Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Both schools currently have access to additional education specific platforms including TeachmateAI and Key GPT as we recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. The schools will treat any use of AI to bully pupils very seriously, in line with our policies. Currently access to these platforms is for adults only.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the schools, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff. The schools are developing a separate AI Policy, working with the Local Authority.

### Acceptable Use of The Internet in Schools

All pupils, parents/carers, 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 federation'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 and restrict access through filtering systems where appropriate. More information is set out in the acceptable use agreements in appendices.

### **Filtering and Monitoring**

The designated safeguarding lead (DSL) (Infants – Kathryn Jesset, Juniors – Katie Thomson) has lead responsibility for filtering and monitoring and works closely with Wavenet to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide ‘appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times. We ensure all staff are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking. They can submit concerns at any point and will be asked for feedback at the time of the regular checks which take place.

Technical and safeguarding colleagues work together closely to carry out reviews and check and also ensure that the school responds to issues and integrates with the curriculum. We carry out half-termly checks to ensure filtering is operational, functioning as expected, etc.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DSL checks filtering reports and notifications monthly and takes any necessary action as a result. At Honeywell School’s we use in-person monitoring in the classroom as well as network monitoring to ensure the safe use of devices.

### **Staff Using Personal Devices Inside School**

All staff who work directly with children should leave their mobile phones on silent and out of view. They should only use them in private staff areas during school hours, these are the staff room, senior manager’s offices or offsite. If a member of staff has a phone issued by the school for school use, this can be used in other areas when appropriate and necessary to do so. This should be for work related purpose only e.g. photographs to record learning.

### **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 can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- 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 by promptly installing the latest updates
- Staff members must not use the device in any way that would violate the school’s terms of acceptable use
- 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 Wavenet.

### **How the Schools 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. 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 schools will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **Training**

### **Staff, governors and volunteers**

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, threatening, 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 up the risks
  - 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 deputy/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.

### **Pupils**

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## **Monitoring Arrangements**

Behaviour and safeguarding issues related to online safety are logged on CPOMs or Arbor which are overseen by the DSLs and Senior Leadership

This policy will be reviewed yearly. At every review, the policy will be shared with the Governing Body. 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.

[childrenscommissioner.gov.uk/our-work/digital/5-a-day/](http://childrenscommissioner.gov.uk/our-work/digital/5-a-day/)



The **digital 5 a day** provides a simple framework that reflects the concerns of parents/ carers as well as children’s behaviours and needs. It can also act as a base for family agreements about internet and digital device use throughout both the holidays and term time.

Based on the NHS’s evidence-based “**five steps to better mental wellbeing**”, the digital 5 a day campaign gives children and parents easy to follow, practical steps to achieve a healthy and balanced digital diet.

### 1. Connect

The internet has enabled everyone to maintain friendships and family relationships no matter where they are in the world and children often say that chatting with friends is the best thing about social media.

It’s important to acknowledge that this is how children keep in touch but it’s also important to have a conversation with them about who they are connecting with and their privacy settings. Remember to keep a dialogue open and talk to your child to understand how they’re spending their time and so that they can come to you for help should they need to.

### 2. Be active

Activity is very important for mental wellbeing and all children should have time to switch off and get moving.

Children don’t have to be an athlete to be active. Find something that they enjoy – be that swimming, walking, dancing or yoga – begin at a level that works for them and make it a regular activity.

Researching an activity or place online before going out is a good way of combining the two and provides an opportunity for you to use the internet together.

### 3. Get creative

The internet provides children with unlimited opportunities to learn and to be creative. From learning to code to building complex structures in Minecraft to creating video content, the summer can be a great opportunity for children to build their digital skills. Time spent online doesn’t have to be spent passively consuming content. It can be educational, creative and can provide opportunities to build skills for later life.

### 4. Give to others

As well as using the internet to learn about how to get involved with local and national charitable schemes, children can give to others through their everyday activities.

Remind children that by giving positive feedback and support to friends and family as well as reporting the negative behaviour of others, children can help the web make a positive place for everyone.

### 5. Be mindful

We hear that children often feel pressured by the constantly connected nature of the internet. While they might want to do other things, it can be difficult for them to put their phones down when apps are encouraging them to engage. Being mindful about the amount of time that your child is spending online – and encouraging them to be mindful about how this makes them feel – is important.

Encourage children to come up with ways of managing this i.e. keeping a diary as way of logging the amount of time they are spending online or downloading an app that helps them manage their notifications.

My name is \_\_\_\_\_ Class \_\_\_\_\_

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:



1. I only **USE** devices or apps, sites or games if I am allowed to.
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused.
3. I look out for my **FRIENDS** and tell someone if they need help.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE**
6. Anything I do online can be shared and might stay online **FOREVER**.
7. I don't keep **SECRETS**  unless they are a nice surprise.
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must. Sometimes these can be dangerous.
9. I don't change **CLOTHES** or get undressed in front of a camera.
10. I always check before **SHARING** my personal information or other people's stories, videos and photos.
11. I am **KIND** and polite to everyone.

|   |
|---|
| ✓ |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |

My trusted adults are:

\_\_\_\_\_ at school  
 \_\_\_\_\_ at home  
 \_\_\_\_\_ at \_\_\_\_\_

I know I can also get in touch with [Childline](#) and get help from **Place2Talk**

My name is \_\_\_\_\_ Class \_\_\_\_\_



#### These statements can keep me and others safe & happy at school and home

1. **I learn online** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. **I behave the same way on devices as face to face in the classroom, and so do my teachers** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. **I ask permission** – At home or school, I only use devices, apps, sites and games if and when I am allowed to. If not sure, I will ask.
4. **I am creative online** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. **I am a good friend online** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. **I am not a bully** – I know just calling something fun or banter doesn't stop the fact that it may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos and if I see it happening, I will tell my trusted adults.
7. **I am a secure online learner** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. **I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. **I know it's not my fault if I see or someone sends me something bad** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. **If I make a mistake, I don't try to hide it but ask for help.**
12. **I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about. I check with a trusted adult before I chat with anyone for the first time, even if they are a 'chatbot'.
13. **I know online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. **I never pretend to be someone else online** – it can be upsetting or even dangerous.
15. **I check with a parent/carer before I meet an online friend** the first time; I never go alone.
16. **I don't go live (videos anyone can see) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
17. **I don't take photos or videos of people without them knowing or agreeing to it** – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult for help if it's safe.
18. **I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. **I can say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. **I follow age rules** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. **I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.



23. *I am careful what I share and protect my online reputation* – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. *I am a rule-follower online* – I know that apps, sites and games have rules on how to behave, and age restrictions. I follow rules, block bullies and report bad behaviour, at home and at school.
25. *I am part of a community* – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it. I talk to others online how I would like to be spoken to.
26. *I respect people's work* – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. *I am a researcher online* – I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across. I will not copy anything without permission. If I am not sure I ask a trusted adult.

**I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:**

**at school that might mean** \_\_\_\_\_

**Outside school, my trusted adults are** \_\_\_\_\_

I know I can also get in touch with [Childline](#), use the **Worry Box in the classroom** or get help from **Place2Talk**

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

### Acceptable Behaviours and Use Agreement (Staff, Governors and Volunteers)



We ask everyone directly involved in the life of Honeywell Schools Federation to sign an Acceptable Behaviours and Use Agreement (ABUA), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media both when on school site and outside of school.



This agreement is reviewed annually, and staff, governors and volunteers are asked to read, understand, follow and sign it when starting at the schools and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. If you have any questions about this AUBA or our approach to online safety, it is your responsibility to please speak to the DSL

#### What am I agreeing to?

- 1. For Staff and Governors Only:** I have read and understood Honeywell Schools Federation full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way (by adults or pupils) to the Designated Safeguarding Lead (if by a child) or Head Teachers (if by an adult) and make them aware of new trends and patterns that I identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'! If I am unsure how to address any issues, I will seek support from the DSLs.
7. I will leave my phone out of view and silenced. Under no circumstances will I use it (or other capture device) in the presence of children, including to take photographs or audio/visual recordings of the schools, its site, staff or pupils. If required (e.g., to take photos of equipment or buildings), I will have the prior permission of the Head Teachers (this may be delegated to other staff) and it will be done in the presence of a member staff. The same principles apply for wearable technology. Smart glasses should not be worn in school. Please speak to the School Business Manager if this presents any issue. There are designated places where mobile phones can be used when not in the presence of children. These are the staff room, senior manager's office or offsite.
8. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
9. For staff only: I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHCE curriculum, both outside the classroom and within the curriculum, supporting subject leaders, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
10. For staff only: When overseeing the use of technology in schools or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
11. I will check with the Head Teachers if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured. This includes any generative AI apps.
12. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods. [onlinesafetyprinciples.lgfl.net](https://onlinesafetyprinciples.lgfl.net)

13. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos). I will flag any concerns about “over blocking” to the DSL (e.g. if I cannot access materials I need in my role).
14. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
15. I will physically monitor pupils using online devices in any area of the school to ensure appropriate and safe use.
16. For staff only: During any periods of remote learning, I will not behave any differently towards pupils compared to when I am in school and will follow the same safeguarding principles as outlined in the Child Protection and Safeguarding Policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
17. I understand that schools’ systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
18. I know the filtering and monitoring systems used within the schools and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the schools to inform regular checks and annual review of these systems.
19. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside the schools, including on social media, e.g., by not sharing other’s images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the schools’ community or not.
20. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways.. I will report any breach of this by others or attempts by pupils to do the same to the Head Teachers.
21. If I am employed by the school and already have a personal relationship to a pupil or their family, I will inform the Head Teachers of this as soon as possible.
22. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy. If I am ever not sure, I will ask first.
23. I will not use any new technology or download any apps without agreement from the Head Teachers
24. I will not use a mobile hotspot to provide internet to any device I use in the schools.
25. I agree to adhere to all provisions of the schools’ Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
26. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
27. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the schools. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this ABUA and/or of the schools’ full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the schools and where appropriate, referral to the relevant authorities.
28. I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation in relation to using these platforms.

### **To Be Completed by The User**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the schools’ most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:**

**Name:**

**Role:**

**Date:**

---



---



---



---

### Acceptable Behaviours and Use Agreement (Parents and Carers)

The use of technology is an essential part of all of our lives. At Honeywell Schools we take our responsibilities for supporting your child to develop skills in using technology very seriously, and their safety and wellbeing are our utmost priority to us. We ask all children, young people and adults involved in the life of Honeywell Schools to read and sign an Acceptable Use Agreement to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). Your child has also signed an acceptable use agreement which can be found in the Online Safety Policy.



We tell your children that they should not behave any differently when they are out of school or using their own device or on a home network. What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online. If you have any questions about this policy, acceptable behaviours and use agreement or our approach to online safety, please speak to the DSL (Infants – Kathryn Jesset, Juniors – Katie Thomson) You can read Honeywell School's full Online Safety Policy on the School's website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc).

#### What am I agreeing to?

1. I understand that Honeywell Junior School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to over block or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I will support my child to follow Honeywell school's policy regarding bringing devices (mobile phones, tablets, Smart watches and glasses etc.) to school. Our school's policy is that Mobile phones, Smart watches and other portable devices are not allowed during the school day. Mobile phones or smart watches which the child uses when travelling alone to or from school must be handed to class teachers at the beginning of the day and they are returned at the end of the day. These devices are stored securely during the day.
7. I understand that my child is able to access learning and communicate with school staff via google classroom (Infant School) or Seesaw (Junior School) in regards to their learning. If they are contacted by someone else or staff ask them to use a different platform to chat, please report this to the Designated Safeguarding Lead (Infants – Kathryn Jesset, Juniors – Katie Thomson) or Head Teachers.
8. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
9. Parents are kindly asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. Children do not have access to their mobiles phones during the school day.
10. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's policy and not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13 years old).

11. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
12. I will follow the school's policy and guidance regarding when I can capture and/or share images/videos. I will **not** share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous (see [nofilming.lgfl.net](https://nofilming.lgfl.net) for more information). The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent.
13. I will not covertly film or make recordings of any interactions with pupils or adults in schools. If I wish to make any recording, we request you to please speak to the Head Teacher of the relevant school.
14. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to [parentsafe.lgfl.net](https://parentsafe.lgfl.net) for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant age - appropriate topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
15. Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks, when appropriate. Find out more at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
16. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
17. I understand that whilst home networks are much less secure than school ones, I can apply safety settings to my home internet and to various devices, operating systems, consoles, apps and games. Find out more at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
18. There are also child-safe search engines e.g. [swiggle.org.uk](https://www.swiggle.org.uk) and YouTube Kids is an alternative to YouTube with age appropriate content. I can also set up SafeSearch to filter explicit content from searches.
19. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, role model healthy behaviours and refer to the principles of the Digital 5 A Day: [childrenscommissioner.gov.uk/our-work/digital/5-a-day/](https://childrenscommissioner.gov.uk/our-work/digital/5-a-day/)
20. I will not attempt to track my child during the school day or on school trips, e.g. with Apple AirTags or similar devices. Not only is this against the terms and conditions of these products, it is unhelpful to the operation of the school, can broadcast the location of children to passing users and can lead to unnecessary distress among parents e.g. if a school trip has an unannounced change of route or schedule.
21. I understand and support the commitments made by my child in the Acceptable Use Policy (AUBA) which s/he has signed, and which can be found in the school's Online Safety Policy, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
22. I can find out more about online safety at Honeywell School's by reading the full Online Safety Policy here, which can be found on the school's website and can talk to my child's class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school. Please also speak to the DSL if you have concerns regarding your child or other children's safety online (Infants – Kathryn Jesset, Juniors – Katie Thomson)

#### **To Be Completed by Parents and Carers**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the schools' most recent online safety / safeguarding policies.

Signature: \_\_\_\_\_

Parent/Carer Name: \_\_\_\_\_

Child's Name: \_\_\_\_\_

Relation to the child: \_\_\_\_\_

Date: \_\_\_\_\_

### Acceptable Behaviours and Use Agreement (Visitors)



Documentation on **SIGN IN APP** and available in hard copy



#### SafeguardED

Visitors and contractors are asked to sign this document before they are allowed access to the schools or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask a member of the office staff. Further details of our approach to online safety can be found in the overall school Online Safety Policy.

If you have any questions during your visit, you must ask the person accompanying you (if appropriate) and/or the School Business Manager. If questions arise after your visit, again contact the School Business Manager.

I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the schools' securities, monitoring and filtering systems and/or viewed by an appropriate member of staff.

1. I will never attempt to arrange any meeting with a pupil, including tutoring session, without the full prior knowledge and approval of the schools, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
2. I will leave my phone out of view and silenced. Under no circumstances will I use it (or other capture device) in the presence of children, including to take photographs or audio/visual recordings of the schools, its site, staff or pupils. If required (e.g., to take photos of equipment or buildings), I will have the prior permission of the Head Teachers (this may be delegated to other staff) and it will be done in the presence of a member staff. The same principles apply for wearable technology. Smart glasses should not be worn in school. Please speak to the School Business Manager if this presents any issue. There are designated places where mobile phones can be used when not in the presence of children. These are the staff room, senior managers office or offsite.
3. If I am given access to school-owned devices, networks, cloud platforms or other technology:
  - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
  - I will not attempt to access any pupil / staff / general school data unless expressly instructed/allowed to do so as part of my role
  - I will not attempt to make contact with any pupils or to gain their contact details under any circumstances
  - I will protect (and not share) my username/password and notify the schools of concerns.
  - I will abide by the terms of the school Data Protection Policy protections
  - I understand that my online activity will be subject to the schools' filtering and monitoring systems, and that any attempts to access content which is illegal or inappropriate for a school setting, may result in further action as per the safeguarding procedures and may result in termination of contract.
4. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the schools.
5. I will not reveal any information on social media or in private which shows the schools in a bad light or could be perceived to do so.
6. I will not do or say anything to undermine the positive online safety messages that the schools disseminate to pupils/students and will not give any advice on online safety issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of '[Using External Visitors to Support Online Safety](#)' from the UK Council for Child Internet Safety (UKCIS). [compiled by experts on the education working group of UKCIS and highly recommended for use.
7. I understand that children can be abused and harmed when using devices and I will report any behaviour (no matter how small) which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Head Teachers (if by an adult).
8. I will only use any technology during my visit, whether provided by the schools or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view any content or material which is or could be perceived to be inappropriate for children or an educational setting. I will not use a mobile hotspot to provide internet to any device I use in schools.

9. If I need to use any specific applications, I must seek authorisation from the School Business Manager before doing so. In particular this includes AI.
10. I will behave in a professional and responsible manner at all times and understand that failure to do so may result in further action being taken and could result in the termination of my contract.

To be completed by the visitor/contractor:

**I have read, understood and agreed to this policy.**

**Signature/s:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Organisation:** \_\_\_\_\_

**Visiting / accompanied by:** \_\_\_\_\_

**Date / time:** \_\_\_\_\_

To be completed by the schools (only when exceptions apply):

**Exceptions to the above policy:** \_\_\_\_\_

**Name / role / date / time** \_\_\_\_\_

#### Appendix 6: Example 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 7: Example ONLINE SAFETY TRAINING NEEDS AUDIT

| 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 behaviour and use agreement for staff, volunteers, governors and visitors? |                                    |
| Are you familiar with the school's acceptable use agreement for pupils and parents/carers?                               |                                    |
| Are you familiar with the filtering and monitoring systems on the school's devices and networks?                         |                                    |
| Do you understand your role and responsibilities in relation to filtering and monitoring?                                |                                    |
| 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?                                  |                                    |