Hayward's Primary School

Online Safety Policy 'ICT and Internet Acceptable Use'

Hayward's Primary School

Written by	Based on a model policy from the key (March 2024)	
Approved by Governors	April 2024	Signed:
Next review due by	Summer 2025	

Contents Page – Online Safety Policy

1. Introduction and Aims of the Policy

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy.

Our school aims 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')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four 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, 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 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 scams

2. 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 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

The Governing Body	The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board 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. The governing board will also 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. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers 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 their safeguarding needs. All governors will: ● Ensure they have read and understand this policy ● Agre and adhere to the terms on acceptable use of the school's ICT systems and the internet ● Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures. ● Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND. This is cause 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.
The Headteacher	The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
The Designated Safeguarding Lead	Details of the school's designated safeguarding lead (DSL) and deputy safeguarding leads are set out in our child protection and safeguarding policy and can be located on our school website.

	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 and governing body to review this policy annually and ensure 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. ● Working with the ICT technician to make sure the appropriate systems and processes are in place ● Working with the headteacher, ICT technician 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's 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 ● Undertaking annual risk assessments that consider and reflect the risks children 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 Technician	The ICT Technician 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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material ● Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly ● Conducting a full security check and monitoring the school's ICT systems on a fortnightly/monthly basis ● Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files ● Ensuring that any online safety incidents are logged (see appendix 5) and are passed on to the member of staff (DSL or Headteacher) to deal with appropriately in line with this policy ● Ensuring that any incidents of cyber-bullying are passed on to the member of staff (DSL or Headteacher) dealt with appropriately in line with the school behaviour policy This list is not intended to be exhaustive. This list is not intended to be exhaustive.
All staff and volunteers	All staff, including contractors and agency staff, and volunteers are responsible for: ● Maintaining an understanding of this policy

	• Implementing this policy consistently • Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use • 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 notifying the Headteacher, DSL and IT technician • Following the correct procedures by speaking with the Headteacher, DSL and IT technician if they need to bypass the filtering and monitoring systems for educational purposes • 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 cyber-bullying are dealt with appropriately in line with the school behaviour policy • Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here' This list is not intended to be exhaustive.
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 (appendix 1) Parents can seek further guidance on keeping children safe online from the following organisations and websites: • What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues • Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics • Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
Visitors and members of the community	Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:
- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

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

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

5. Educating parents about online safety

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

Where relevant, online safety will also be covered during parents' evenings.

School will let parents/carers know:

- What systems the school used 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 school, if anyone, their child will be interacting with online.

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 and/or IT Coordinator.

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

6. Online Abuse

Preventing and addressing online bullying

Our pupils increasingly use electronic equipment on a daily basis to access the internet and share content and images via social media sites such as facebook, twitter, instagram, snapchat and oovoo.

Unfortunately, some adults and other children use these technologies to harm children. The harm might range from sending hurtful or abusive texts or emails, to grooming and enticing children to engage in sexual behaviour such as webcam photography or face-to-face meetings. Pupils may also be distressed or harmed by accessing inappropriate material such as pornographic websites or those which promote extremist behaviour, criminal activity, suicide or eating disorders
To help prevent online 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 online bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss online bullying with their tutor classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online 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 online bullying, its impact and ways to support pupils, as part of safeguarding training).

The school also sends information/leaflets on online 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 online 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.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher **or** DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher or DSL 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.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial Intelligence (AI)

Generative artificial intelligence (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 Bard.

Hayward's recognises 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.

Hayward's will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet

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

Use of the schools' internet must be for educational purposes only, or for the purpose of fulfilling the duties 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.

8. Pupils using mobile devices in school

Mobile phones will not be used in the classroom. Any mobile phones brought in from home will be stored in the school office for safety.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside of 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 by always installing the latest updates

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

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

10. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff 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 that 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, 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.

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 the appendix.

This policy will be reviewed bi-annually. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: 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: ● Ask a teacher or adult if I can do so before using them ● Only use websites that a teacher or adult has told me or allowed me to use ● Tell my teacher immediately if: ○ I select a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends ● Use school computers for school work only ● Be kind to others and not upset or be rude to them ● Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it **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, 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. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** ● Always use the school's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my usernames and passwords safe and not share these with others ● 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 ● Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others ● Always log off or shut down a computer when I've finished working on it **I will not:** ● 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 ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate ● Log in to the school's network using someone else's details ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** ● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **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: ● 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) ● Use them in any way that could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of pupils without checking with teachers first ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● 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. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT technician know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 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/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?	

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**

Parental permission letter for g suite for education

Dear Parents and Carers,

Computing at Hayward's Primary School is about to change.

We have recently taken the decision to incorporate **G Suite for Education** into our curriculum, which will see every child in the school have their own personal cloud computing space, accessible from any internet enabled device. They will have their own virtual hard drive and be able to use a raft of **Google** programs that will help them research, produce work and collaborate and communicate with classmates and teachers. It will also give the children the ability to access learning and complete work from home. We are seeking your permission to provide and manage an account for your child.

The account will include apps such as

- **My Drive** (virtual hard drive where all work is automatically stored)
- **Gmail** (completely controlled by the school)
- **Google Docs** (Google version of Word)
- **Google Slides** (Google version of Powerpoint)
- **Classroom** (portal to communicate with teacher and complete class work)
- **and more** - we will add apps as and when they are needed or become available

G suite is used and trusted by **tens of millions** of students, teachers and businesses around the world. It is an exciting journey to be starting and at Hayward's, students will use their G Suite accounts to complete assignments, communicate with teachers, sign into Chromebooks and learn 21st century digital citizenship skills.

Safety is an absolute necessity at Hayward's. The school will have **comprehensive control** over **all** aspects of the system, and we will be introducing it to the children in stages, building up the skillset to use it step by step. Time is taken in every computing lesson to promote responsible computer use and address staying safe online and we will be monitoring pupil's accounts and conducting spot checks to make ensure pupils are using it correctly.

You will naturally have many questions about this new system. The accompanying PDF document sent out via parentmail aims to provide answers to common questions about what sort of information will be stored, and what Google can and can't do with that information. Please read it carefully and if you have any questions at all, please ask.

If you are happy, **please sign below** to indicate that you've **read the notice** and **give your consent**. Permission will last for your child's entire time in Hayward's Primary school and accounts will be deleted within 6 months of them leaving the school. If you don't provide your consent, we will not create a G Suite for Education account for your child. They will still have access to the school computers and learnpads, but will not be able to collaborate with their peers or join us on the computing journey the school needs to take.

Thank you,
Mr Smith

- -

I give permission for Hayward's Primary School to create/maintain a **G Suite for Education** account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below. I understand this permission will last for my child's entire time as a Hayward's Primary School pupil.

_____
Full name of student

_____
Printed name of parent/guardian

_____ _____
Signature of parent/guardian Date

G Suite for Education Notice to Parents and Guardians

G Suite for Education is a great platform designed entirely to enhance a child's familiarity with computing, and is an ideal tool for this increasingly digital world. The children will be able to access it in school and at home, and will build up skills that will last them a lifetime. As it has been designed with children's education in mind, it **is not** a platform for Google to collect information, and they do not use it as such. In creating an account for the children, we use only their name, which is obviously needed for personalisation, and class, which is needed for the organisational structure. No other information has been used.

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may have access, and use, the following "Core Services" offered by Google. Access to all programs is **strictly controlled** by the school and most will only become available if the children need to use them during lessons. The apps **in bold** are available for the children to use always. The others will be available if needed.

- **Gmail** (children can only send and receive e-mails to and from others with the haywards.org domain name unless it is part of a unit of work. All e-mails can be checked by the school)
- Google+
- **Calendar**
- **Chrome Sync** (allows children to work on different chromebooks seamlessly)
- **Classroom** (communication with teacher and class)
- Cloud Search
- Contacts
- **Docs, Sheets, Slides, Forms** (the Google equivalent of Microsoft Office apps)
- **Drive** (Children's personal hard drive where they store their work)
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk (Social networking and collaboration tools. Not currently enabled. If and when they are, they will be monitored closely and used internally only)
- Jamboard
- Keep
- Sites
- Google Earth
- Vault

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Hayward's may provide Google with certain - very limited - personal information about the student, including, for example, a name, email address (haywards.org domain name), and password.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;

- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google **does not** serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Does Google use student personal information for users schools to target advertising?

No. For G Suite for Education users in primary and secondary schools, Google **does not** use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others in the school, allowing them to work collaboratively on the same document. Occasionally, if it is part of a unit of work, creations by the students may be shared publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google **will not** share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent which may be obtained through G Suite for Education schools.
- With Hayward's Primary School. G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. **If you don't provide your consent, we will not create a G Suite for Education account for your child**, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting the school. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, **please contact Mr Gordon**. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html) [if school/district has accepted the Data Processing Amendment (see https://support.google.com/a/answer/2888485?hl=en), insert: and the Data Processing Amendment (at https://www.google.com/intl/en/work/apps/terms/dpa_terms.html)].