Hayward's Primary School

'ICT and Internet Acceptable Use'

Hayward's Primary School

Written by	Based on a model policy from the key (April 2026)	
Approved by Governors	Summer 2026	Signed:
Next review due by	Summer 2027	

Contents

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.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our disciplinary policy.

2. Legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

● **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

● **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

● **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 5 for a glossary of cyber security terminology.

4. Unacceptable use of the internet

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and the school's staff code of conduct..

Copies of the school's behaviour policy and policy on online safety and mobile phone and small technology can be found on the www.haywards.org website. The staff code of conduct can be found in the relevant GDrive.

4. Expectations of Staff

Expectations of Staff (including Governors, Volunteers and Contractors)	
Access to school ICT facilities and materials	The school's ICT Technician manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to: ● Computers, tablets, and other devices ● Access permissions for certain programmes or files Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities. Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT technician
Use of School Supplied Equipment	School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must: ● Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality ● Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations ● Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device ● Lock devices with a password when unattended. Passwords must: ● Not be shared with others and must be changed regularly ● Be suitably strong, in accordance with the school's password policy (see section [8.1]) ● Not be reused across multiple accounts ● Update software, operating systems and applications when prompted, or as directed by the ICT technician ● Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks ● Report any loss, theft, damage or compromise of a school device promptly to the ICT technician, designated safeguarding lead and data protection officer

Use of phones and email	The school provides each member of staff with two email address - @haywards.devon.sch.uk and @haywards.org. These email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s). All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable. Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure. Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4. All staff are only allowed to use mobile phones in designated areas of the school e.g. the car park, headteacher's office, staff room, business manager's office or main office. Mobile phones capable of photographing children should not be out in the classroom. Such personal equipment must not be used at any time during contact with pupils. Photographs/still images or video footage of pupils should only be taken using school equipment, for purposes authorised by the school. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be stored in accordance with the school's procedures, on school equipment. Mobile phones and personal cameras should not be used in school. Use of 365 login – staff are required to use Office 365 email APP on mobile phones and other mobile devices. Staff need to ensure that there phones are locked and appropriately password protected. Care should be taken to ensure that school documents are not downloaded onto the phone and if they are they are immediately when read.

Personal use	Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher may withdraw or restrict this permission at any time and at their discretion. Personal use is permitted provided that such use: ● Does not take place during teaching hours ● Does not constitute 'unacceptable use' ● Takes place when no pupils are present ● Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken. Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy. Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices. Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them. Staff should take care to follow the school's guidelines on use of social media contained within the Code of Conduct to protect themselves online and avoid compromising their professional integrity. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT technician. Staff will keep all confidential documentation in the encrypted drive that has been provided for them on their individual laptops and confidential documentation on an approved, encrypted memory stick, provided by the school.

Personal Social Media Accounts	Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. When staff are using social networking and personal publication (also found in our Code of Conduct Document which is signed by staff each year): ● Staff should be extremely cautious when using social networking sites outside of work and avoid publishing, or allowing to be published, any material, including comments or images, that could damage their professional reputation and/or bring the school into disrepute. Where staff do use social networking sites it is strongly advised that profiles should be set as 'private' and under no circumstances should staff allow access to pupils, their families and or carers. Staff should not publish information or photographs about their work in school. If 'friending' parents online, staff should be mindful of the potential dangers of personal information coming into the public arena. We recommend that staff consider friendship requests from members of the school community, outside fellow staff, very carefully. Staff should not publish information or photographs about their work in school. ● Employees must exercise caution in their use of all social media or any other web-based presence that they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others. This may also include the use of dating websites where employees could encounter pupils either with their own profile or acting covertly. ● Employees must not link themselves with the school on any social network site they use unless with prior consent of the Headteacher. ● Employees must only contact pupils via school-authorised mechanisms. At no time should personal telephone numbers, email addresses or communication routes via personal accounts on social media platforms be used to communicate with pupils. ● Employees must not use equipment belonging to the school to access pornography; neither should personal equipment containing pornographic images or links to them be brought into the workplace. Doing so will raise serious concerns about the suitability of the employee to continue to work in schools. ● Employees must not respond to negative comments about the school or its staff posted online but bring this to the attention of the Headteacher. ● Employees must report to the Headteacher any contact by a pupil by an inappropriate route. Any communications made in a professional capacity through social media must not either knowingly or recklessly: ● place a child or young person at risk of harm; ● bring the school into disrepute; ● breach confidentiality; ● breach copyright; ● breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: ● making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; ● using social media to bully another individual; or posting images that are discriminatory or offensive or links to such content

Monitoring and filtering of the school network and the use of ICT facilities	To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of: ● Internet sites visited ● Bandwidth usage ● Email accounts ● Telephone calls ● User activity/access logs ● Any other electronic communications Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes. ● To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy ● To find lost messages or retrieve messages lost due to computer failure ● To help in the investigation of alleged wrongdoing ● To comply with any legal obligation The list above is not exhaustive. The school monitors ICT use in order to: ● Obtain information related to school business ● Investigate compliance with school policies, procedures and standards ● Ensure effective school and ICT operation ● Conduct training or quality control exercises ● Prevent or detect crime ● Comply with a subject access request, Freedom of Information Act request, or any other legal obligation Our governing board is responsible for making sure that: ● The school meets the DfE's filtering and monitoring standards ● Appropriate filtering and monitoring systems are in place ● Staff are aware of those systems and trained in their related roles and responsibilities ● For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns ● It regularly reviews the effectiveness of the school's monitoring and filtering systems The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Expectations of Pupils

<table>
<tr><th colspan="2">Expectations of Pupils</th></tr>
<tr><td rowspan="2">Access to ICT facilities</td><td>Pupils have access to the following ICT equipment and facilities whilst at school:
● Chromebooks are available to use in the lessons under the supervision of their class teachers.

Pupils will have access to the following learning sites and have their own user names and password for access:

● Google (through the G Suite for Education Package)
● Timestable Rock Stars
● Accelerated Reader
●</td></tr>
<tr><td>G suite for education

The school has implemented Google’s package of apps designed for use in schools; g suite for education. Under the domain name of @haywards.org, the collection of apps work together and promote collaborative learning. Each pupil will be given their own account, with access to their own bank of apps, primarily:

● Gmail
● Classroom
● Docs, Sheets, Slides, Forms - the Google equivalent of Microsoft Office apps
● Drive - personal hard drive where they store work

Pupils will be able to access their accounts both in school and at home, dependant on parental permission – see appendix 5 for letter, which includes details of information gathered by google and their policy on advertising.

Staff members will also be given their own account, which includes access to further apps such as:
● Calendar
● Gmail
● Google Hangouts
● Google Meets
● Jamboard
● Sites
● Google Earth

Access to every app is strictly controlled by the ICT Technician and is granted on a needs basis. Pupils can be granted access to these apps, but it will be only temporary and within the context of classroom learning, and under the supervision of the classroom teacher.</td></tr>
</table>

Unacceptable use of ICT and the internet outside of school	The school will sanction pupils, in line with the school's Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises): ● Using ICT or the internet to breach intellectual property rights or copyright ● Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination ● Breaching the school's policies or procedures ● Any illegal conduct, or making statements which are deemed to be advocating illegal activity ● Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate ● Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery) ● Activity which defames or disparages the school, or risks bringing the school into disrepute ● Sharing confidential information about the school, other pupils, or other members of the school community ● Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel ● Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities ● Causing intentional damage to the school's ICT facilities or materials ● Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation ● Using inappropriate or offensive language

7. Expectations of Parents and Carers

Expectations of Parents/Carers	
Access to ICT facilities and materials	Parents/carers do not have access to the school's ICT facilities as a matter of course. However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion. Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online	We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels. We ask parents/carers to sign the agreement in appendix 2.
Communicating with parents/carers about pupil activity	The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared. In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any incoming files should always be virus-checked before they are downloaded.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection
All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials
All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT Technician.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Technician and the Data Protection Officer (DPO) immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Locking laptops/workstations using "Windows key L" will do this immediately. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption
The school makes sure that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT technician.

9. Protection from cyber attacks
The school will:
● Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
● Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

- The methods hackers use for tricking people into disclosing personal information, including phishing
- Online safety and password security
- Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- The physical security of devices, for example not leaving a laptop unlocked and unattended
- The risks of using removable storage media, such as USBs
- Multi-factor authentication
- How and when to report a cyber incident or attack
- How and when to report a data breach
- Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
- How to check the sender address in an email
- How to respond to a request for bank details, personal information or login details
- How to verify requests for payments or changes to information

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure

- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:

Proportionate: the school will verify this using a third-party audit (such as TME) annually, to objectively test that what it has in place is effective

Multi-layered: everyone will be clear on what to look out for to keep our systems safe

Up to date: with a system in place to monitor when the school needs to update its software

Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be

- Backup critical data daily and store these backups on server (daily) and a backup is made up of that weekly and is stored securely within school. Lots of critical information is held on GDrive which is a cloud-based backup which is encrypted.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT technician
- Make sure staff:
- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Make sure effective cyber breach prevention measures and processes are in place
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually by the IT technician and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event.
- Appoint a digital lead to oversee cyber risk assessment.

10. Internet Access

The school's wireless internet connection is secure. Filtering and monitoring is used to ensure that inappropriate sites are filtered. Staff are aware that should an inappropriate site appear they are required to immediately report it to the IT manager.

10.1 Pupils

Pupils can access WiFi throughout the school through school based computers which have appropriately filtering systems in place. Pupils will not be allowed to access the school WiFi through their own personal devices.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:
- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and Review arrangements

The Headteacher or 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 annually. At every review, the policy will be shared with the governing board.

The governor board is responsible for review/approving this policy.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Online Safety Policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Pupil and Parent Carers Acceptable Use Agreement

This will be completed by families online.

● 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 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, 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 ● 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 understand 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 close/lock my device when leaving it unattended. I will ensure that all devices including interactive classroom screens are switched off at the end of the day and that plugs/leads are not left switched on with no device attached. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will inform the Headteacher or the designated safeguarding lead (DSL) if a pupil contacts me through inappropriate means I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

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

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

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 5: 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)].