Henleaze Junior School

Online Safety Policy

Review

Review Cycle	Date of Current Policy	Author(s) of Current Policy
Annual	Term 2, 2023	Term 2, 2024

Contents

Equalities Statement

We are committed to anti-discriminatory practice and recognise children and families' diverse circumstances. We ensure that all children have the same protection, regardless of any barriers they may face. With regards to safeguarding, we will consider our duties under the Equalities Act 2010 in relation to making reasonable adjustments, non-discrimination and our Public Sector Equality Duty.

Safeguarding statement

Henleaze Junior School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment, in accordance with the school's Safeguarding Policy.

Aims

Our approach to online safety is based on addressing the following four key categories of risk:

1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. 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
3. 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
4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

At Henleaze Junior School we aim to:

- Provide internet access expressly for educational use and include filtered material content appropriate to pupils, staff, volunteers and governors.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department'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.

This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

Trustees

The board of trustees has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The trustee with responsibility for safeguarding will liaise with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of the Acceptable Use Agreement for Staff, Governors, Visitors and Volunteers (AUA)
- Ensure that, where necessary, teaching about online safety is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a "one size fits all" approach may not be appropriate for all children in all situations.

Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Online Safety Lead

The Online Safety Lead takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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
- Liaising with other agencies and/or external services if necessary.

This list is not exhaustive.

ICT Support Contractor

The ICT support contractor is responsible for:

- Ensuring that the school technical systems are managed in ways that ensure that the school meets recommended technical requirements
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not exhaustive.

Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices

- They have read, understood and signed the Acceptable Use Agreement for Staff, Governors, Visitors and Volunteers (AUA)
- All members of the school are responsible for reporting any online safety issues, and recording them on CPOMS. Staff will also be asked at each staff meeting if there are any online safety issues to be discussed. The Headteacher will keep a record of any online safety issues and deal with accordingly following the 'Online Safety Response Grid and Flow Chart' This will be done in conjunction with the Online Safety Lead Teacher and/or the Online Safety Lead Trustee.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Acceptable Use Agreement for Pupils (AUA)
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

This list is not exhaustive.

Volunteers and visitors

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 Acceptable Use Agreement for Staff, Governors, Visitors and Volunteers (AUA)

All volunteers and visitors are expected to tell a member of staff if they see or hear anything that concerns them.

Parents and Carers

Are responsible for ensuring that they:

- 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 of the Acceptable Use Agreement for Pupils (AUA)
- Ensure their child has understood and agreed to the terms of bringing a mobile phone to school where this is relevant
- Follow school policy on taking photograph and films during school events
- Complete the consent form for the use of images and video of children in various contexts
- Monitor their child's online activities outside of school and alert a member of staff if they see or hear anything that concerns them.

When children start at Henleaze Junior School, parents/carers will receive a parental consent form which includes an explanation of how the school may use video, sound and images for internal and external publication. Every parent must complete this form to show agreement and consent.

The school will help parents understand online safety issues through regular guidance in the HJS Update, on the Online Safety Resources page on the school website and from time to time through face to face information meetings with experts in the field.

Pupils

Pupils will be expected to:

- use the school digital technology systems in accordance with the Acceptable Use Agreement for Pupils (AUA)
- understand and agree to the terms of bringing a mobile phone to school where this is relevant
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the taking / use of images and on cyber-bullying.
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Educating pupils about online safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupils will be taught about online safety as part of the curriculum, ensuring coverage in line with the recommended framework 'Education for a Connected World'. The curriculum for online safety is published on the Online Safety page on the school website.

We provide key online safety messages that are reinforced as part of a planned programme of assemblies and other activities

Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

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
- To be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- To acknowledge the source of information used and to respect copyright when using material accessed on the internet

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Training

Staff members will receive training on safer internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher safeguarding training at least once each academic year, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

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

Training will also help staff:

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

The DSL and DDSLs 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 updates on safe internet use and online safeguarding issues.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring

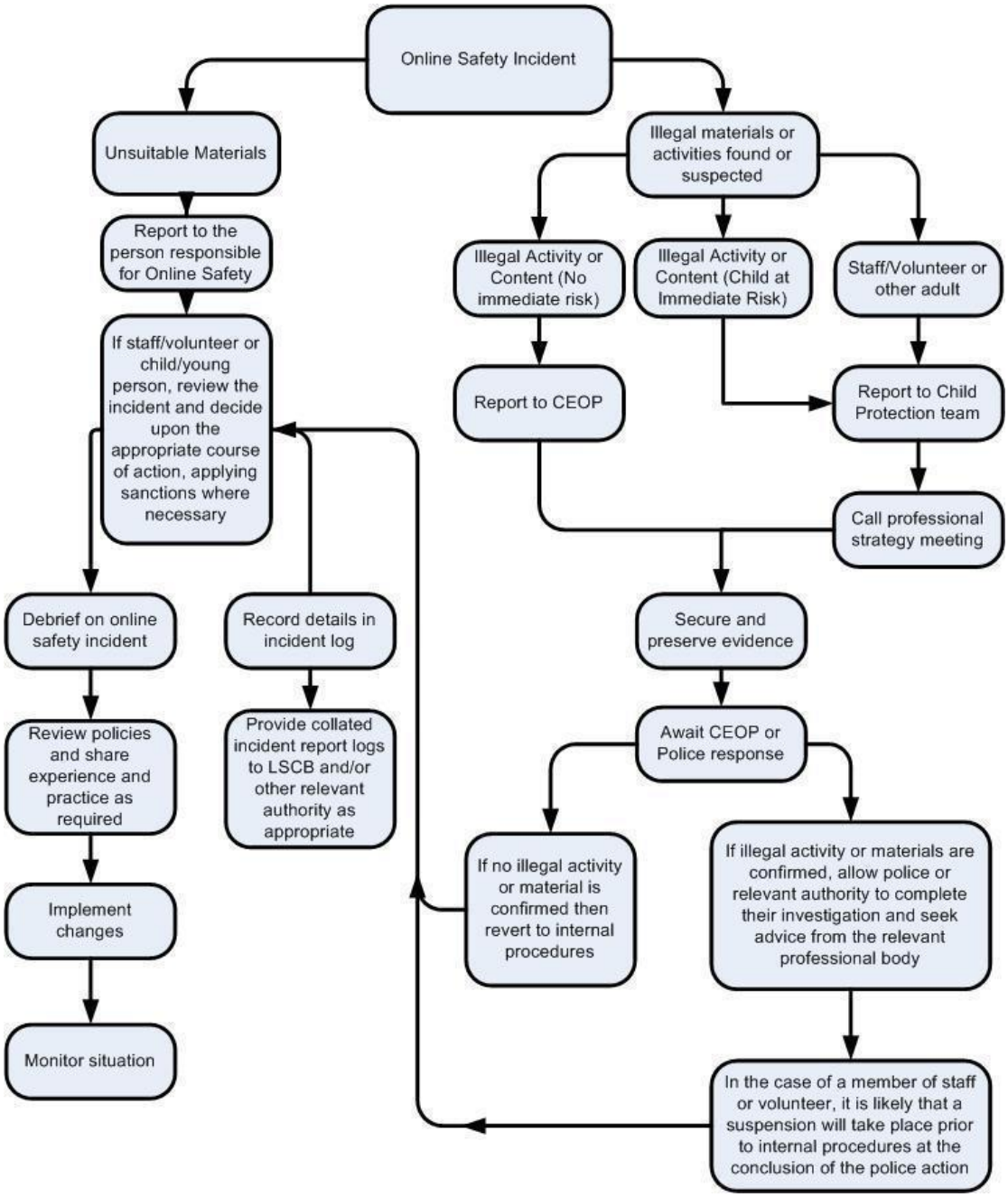
The school logs behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed annually as part of the review of Safeguarding procedures and the KCSIE document, in collaboration with the Online Safety Lead. At every review, the policy will be shared with the governing board.

Appendix A

Response to misuse

In the event of any action that breaks our Acceptable Use Agreements or any of the unsuitable/inappropriate activities listed below, we will respond in accordance with the flow chart.



Inappropriate activity may include any use of games or websites, including social media sites outside of school, which are not age appropriate and any material such as films that are not age appropriate, which would be a safeguarding issue.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils	Actions / Sanctions							
Incidents: *This includes incidents that happen outside school if they have an impact inside school. X = definite action P = possible action	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X				P		X	
Unauthorised use of social media / messaging apps / personal email	X	P			X	P	X	
Unauthorised downloading or uploading of files	X	P			P	P	X	
Allowing others to access school / academy network by sharing username and passwords	X				P	P	X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X				P	P	X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X		X	X	X		X
Corrupting or destroying the data of other users	X	X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	P		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X		X

Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	P	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X					X	X	

Staff, governors and visitors and volunteers	Actions / Sanctions						
Incidents: *This includes incidents that happen outside school. X = definite action P = possible action	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X		X	X
Inappropriate personal use of the internet / social media / personal email	X				X	P	P
Unauthorised downloading or uploading of files	P			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	P				X		P
Careless use of personal data eg holding or transferring data in an insecure manner	P	P			X	P	P
Deliberate actions to breach data protection or network security rules	X	P			X	P	P
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X			P	P
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	P		X	P	P
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	P		X	P	P
Actions which could compromise the staff member's professional standing	X	P			X	P	P

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	P			X	P	P
Using proxy sites or other means to subvert the school's / academy's filtering system	X			X	X	P	P
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X	P	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X
Breaching copyright or licensing regulations	P				X		P
Continued infringements of the above, following previous warnings or sanctions	X	P				X	P

Appendix B

Cyberbullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

Within the whole school approach to online safety everyone will be aware of the breadth of issues to be addressed using the four C categories outlined in KCSIE (see appendix 6) including that of peer on peer abuse.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils as part of their learning around online safety.

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

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

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Appendix C

Use of school devices

Staff

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 manager.

Any hard copy data (e.g. pupil records, planners, diaries etc) taken offsite must be suitably secured in both transit and at rest. For example, ensuring it is not on display when left in a vehicle - leaving documents in a vehicle overnight is not acceptable, and ensuring it is either locked away or out of sight when working from home.

Use of own devices

Pupils

Pupils may only bring mobile devices into school on the condition that they are:

- Switched off at all times whilst on the school grounds
- Handed in to the class teacher at the beginning of the day and only collected at the end of the school day

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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.

Staff

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) to securely access some or all of the school's systems, applications and services.

The following conditions apply to the use of this facility.

- Staff may only connect to the school's systems for the purpose of authorised work or their studies.
- Ideally use of a device that has access to the school's systems, applications and services via the BYOD facility should be limited to its owner and should not be shared. If it is necessary to share a device, the first user must ensure that they are logged out of their school account before handing over the device to a colleague/friend.
- Account logon, passwords and pin numbers for gaining access to the school's systems, applications and services that have been issued to individuals must remain confidential and never shared with others.
- No data from the school system may be downloaded and saved to a device. Similarly, data and information may not be downloaded to any storage device, such as a USB memory stick, that is attached to the BYOD device that has been granted access. Staff should be conscious of where they

are using their device. They should ensure data and systems displayed on the screen of the device are not visible to others. Screenshots of systems must not be taken.

- Personal devices are brought into the school entirely at the risk of the owner. The school does not accept any liability for loss or damage of personal devices and data that are using the BYOD system. It is recommended that the owner (at their own expense) purchases an insurance policy to cover loss / theft / damage etc.
- The school accepts no responsibility for the day-to-day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the school's network or whilst resolving any connectivity issues.
- The school recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the school.
- Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.
- Any charges relating to connecting a BYOD device to the school's systems, applications and services, such as using the data element of a mobile phone contract, are the responsibility of the device owner. It is recommended that Staff using mobile data or Wi-Fi hotspots should periodically monitor the flow of data to ensure that they have sufficient allowance. The school accepts no responsibility for the data required to provide those applications and services.
- While the school will take every precaution to prevent an employee's own data from being lost when the school needs to 'remote wipe' a device, it is the employee's responsibility to take precautions to protect their data and information, such as backing up emails, contacts, etc
- Confidential data should only be accessed for a specific work-related requirement.
- Printing hard copies of material containing personal data is strongly discouraged as it will create security and destruction issues.
- Hard copies may only be disposed of at school in confidential waste / via school shredders).
- Staff must not use their own devices to take images or footage of students. Only school equipment may be used, and images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
- Staff should not save the personal numbers of students to their devices and should use trip phones where appropriate.
- Passwords must not be saved, either in a web browser on the device or written down and left in accessible places.
- Users must log out of programmes when they are no longer using them.
- The device may be remotely wiped if:
    - The device is lost
    - When a member of staff leaves the school
    - IT detects an incident, such as a data breach or a cyber incident, that presents a threat to the school's systems, applications and services.

In the case of data loss staff / students must immediately inform the School Business Manager if:

- Their password has been breached
- Their device is lost or stolen
- Organisational systems are not working normally - in those cases Bristol ICT support may choose to wipe data from the device in order to minimise risk of an impact on either the school's systems, applications and services.

Appendix D

Use of digital and video images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers must only use school IT equipment to take digital / video images and this must be to support educational aims. They must follow school policies concerning the sharing, distribution and publication of those images.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Anyone publishing images is required to refer to the consents provided by parents when children are admitted to the school.

All parents/carers are required to complete a Consent Form for the Use Of Photos and Videos when their child is admitted to school. Details of consents given are kept on the school's management of Information System and are referred to before use of any images.

Appendix E

Online learning platform

All children are given a Microsoft Teams account an admission to the school. Teams is used as the principal form of home-school communication between teachers and their pupils.

We have set passwords which children do not have to change. School staff have access to a master copy of all the passwords. If children forget their password, they should ask their class teacher, or a member of the school office staff, for a reminder.

We have set the accounts up for the children, but we encourage parents to take joint ownership of the account and to supervise their children's activities online. We see this as an important and exciting enhancement to our ways of communicating between home and school, enabling parents to engage actively with their children's learning.

Accessing your account

You can access Teams from any web browser by going to teams.microsoft.com.

For the best experience, download the Teams app onto your computer or tablet or phone.

If your child has their own device, or if they are using a device that is not used by another family member for Teams, they may stay logged into their account for quick access. However, please note, you cannot access another person's Teams. If a parent uses Teams for work, they would have to log out in order for their child to log in. If siblings share the same device at home, they have to log out of one account in order to log into another one.

Your teams

Each child is a member of 2 Teams:

- Their class Team. All the teachers in their year group and all of the children in their class can see everything that is posted in this Team.
- Their year group Team. Every child in the year group is a member of that team, and all of the teachers and learning support assistants who work in the year are supervisors, as well as Mr Barber, who oversees all of the teams.

The General Channel

Only supervisors can post on this channel. This is where we will put important messages that the class or the whole year group need to see. It might be a homework task, or a reminder about something happening next week.

In the Files tab, there are folders for each subject. Teachers will upload the main lesson plans each week so that children can talk about what they have been learning at home and parents can follow up if they wish with further practice.

Class Chat Channels

We have set these up in Years 5 and 6. Children are able to initiate conversations on this channel and respond to each other.

Chat

The Chat function enables children to engage in private conversations with their teacher. This can be used to raise worries or concerns or to make suggestions that children do not want to raise in front of the rest of the class.

The same function enables children to start a conversation with anyone else with a Henleaze Junior School account. They may wish to use this to ask a friend to remind them about a homework task, or to collaborate with a group of friends on a project. They should not use this facility as a social network or for gaming.

We teach children how to use Chat responsibly, and how to show kindness and respect in their online conversations. Since Chat messages are private, teachers do not read them unless any inappropriate use is brought to our attention by children, parents or colleagues.

Although children's Chat messages are private, and we respect their privacy, if we have any reason to believe they are using Chat inappropriately, we will log into their account to check their activity. We will speak to them and their parents about expected behaviour online, and will monitor their account. In extreme circumstances, we may turn off the Chat function for an individual who is not behaving kindly or responsibly.

Teams Manners

Children are expected to behave in Teams exactly as they are expected to behave in school: treating each other with respect, taking their learning seriously, and sticking to the topic. If it would not be appropriate to say something in the classroom, it is not appropriate to say it in Teams.

We will teach them how to use "conversations" in Teams to reply to questions that the teachers post, sticking to the subject being discussed.

We know that some children get very excited about typing messages to their friends and using emojis and LOLs. We will remind them that everyone, including the staff, can see everything that is posted and we are sure that they will use the channels responsibly.

When a teacher posts a topic for discussion, children will be able to respond by hitting "Reply".

Parents are asked to supervise their children's online activities, including their use of Microsoft Teams. If parents notice any inappropriate posts, they should talk to their child and inform the school.

How to use Teams for polite conversation

1. Always be respectful and sensible when you write in Teams.
2. Stick to the subject being discussed.
3. Click Reply to respond to a conversation.
4. Don't post pointless messages or emojis.
5. Don't use Teams to have personal conversations with your friends – remember it is a school account, for school work and messages.
6. Remember that all the children and all the school staff can see everything you write on the Channels and Chats in Teams. (That includes Mr Barber).
7. Remember that your parents also know your password, and they will be keeping an eye on what you write.