	IT & Acceptable Use Policy Updated: 09-25 Next Review: 09-26 Prepared by: RYB/PAW/JOH Authorised by: TZL

This Policy applies throughout the School from the EYFS to Year 6.

Introduction

This Policy applies to all members of the School community who use School IT systems, as a condition of access. Access to School systems is not intended to confer any status of employment on any contractors or service providers.

The DSL has lead responsibility for online safety, including oversight of filtering and monitoring, incident response, staff training, and ensuring online safety is integrated into the curriculum. Governors and the Senior Leadership Team review filtering and monitoring arrangements at least annually, in line with KCSIE. The School will use the DfE's "Plan Technology for Your School" tool to assess and strengthen its filtering and monitoring systems.

The computer system is owned by the School. 'The computer system' means all computers, iPads, phones and other associated equipment belonging to the School, whether part of the School's integrated network, stand-alone or taken off-site.

Professional use of the computer system is characterised by activities that provide pupils with appropriate learning experiences and allow adults to enhance their own professional development. The School recognises that technologies such as the internet and email will have a profound effect on pupils' education and staff professional development in the coming years and the School's Online Safety Policy has been written accordingly.

All pupils must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of internet use. They must sign an acceptable use statement agreeing to the highlighted points (see Appendix).

Online safety is also explicitly taught through the Computing and PSHE curriculum, assemblies, and other opportunities, covering age-appropriate issues such as cyberbullying, online privacy, misinformation, radicalisation and emerging risks (including generative AI and deepfakes). This includes teaching pupils how to identify and challenge misinformation, disinformation, and conspiracy theories, in line with KCSIE.

If staff are accessing the internet via their own data contracts on their own devices for personal use, then the same internet access rules apply when staff are on School premises. Mobile phones may only be used in the staffroom, in offices which are not frequented by children, or in areas of the school which are at that time not frequented by children and to which children have no access. Mobile phones may be used when there are no children on the premises

Online behaviour

All internet activity should be appropriate to staff professional activities or the pupils' education. As a member of the School community, you should follow these principles in all your online activities:

- The School cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Staff should ensure that online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, sexually explicit or promotes violence, discrimination or extremism, or raises safeguarding issues)
- Access to websites that could be categorised as "adults only" is not permitted
- Respect the privacy of others. Do not share photos, videos, contact details or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission
- Do not access or share material that infringes copyright. When using downloaded materials, including free materials, the intellectual property rights of the originator must be respected and credited. All material saved on the School's network is the property of the School and making unauthorised copies of materials contained thereon may be in breach of data protection law[1], individual copyright or intellectual property rights
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others or carry out illegal activities
- Use of the School's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited

Using the School's IT systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access School IT systems using your own username and password. Do not share your username or password with anyone else
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access
- Do not attempt to install software on, or otherwise alter, School IT systems
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above
- Remember that the School monitors the use of the School's IT systems and that the School can view content accessed or sent via its systems
- All internet activity, including searches conducted on platforms such as Google, Bing, and YouTube, will be logged and monitored by the filtering system. This system tracks both staff and student usage to ensure compliance with acceptable use policies. System administrators will regularly review these logs, which include search queries, website visits, and other online behaviour, to ensure appropriate internet use and maintain network security
- Do not sign into your personal email accounts on school devices

[1] General Data Protection Regulation (EU 2016/679), the UK Data Protection Act 2018 and related legislation, The Privacy and Electronic Communications Regulations 2003 and the Protection of Freedoms Act 2012.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They must contain a minimum of 12 characters made up of letters, numbers and symbols. They should not be obvious (for example password 123456, a family name or birthdays), nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password or keep a list of passwords where they may be accessed, and must change a password immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. Staff will be automatically prompted to change their password every 6 months.

It is the responsibility of the user to ensure that they have logged off the system when they have completed their task.

Pupil email addresses (without access to email functionality) are issued at the beginning of each academic year and recorded in their homework, reading diaries and are sent to the parents via iSAMS email. Members of staff can locate a child's email address via iSAMS. These addresses are used solely for logging into online services, such as Google Classroom, and are distributed to all pupils for this purpose.

Pupil passwords are changed annually and pupils are encouraged to keep these confidential. Staff have lists of pupil details to support quick sign-on, but these are kept away from pupils.

Use of School property

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager.

The School provides portable computing equipment such as laptop computers iPads to enhance the pupils' education and to allow staff to make efficient use of such equipment to enhance their own professional activities. The same principles of acceptable use apply to portable equipment.

Once equipment has been used, it should be returned to the resource area, put away in its correct order and put on charge, ready for future use.

If equipment such as iPads is taken offsite for use by staff in accordance with this Acceptable Use Policy, the member of staff would bear responsibility if equipment is lost or damaged. Please make sure to contact the IT Manager before taking an iPad offsite to make sure a password is added to the device.

Where a member of staff is likely to be away from School through illness, professional development (such as training, secondment etc.,) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to School. In the event of illness, it is up to the School to collect the equipment if the individual is unable to return it.

If an individual leaves the employment of the School, any equipment, must be returned before or on their last day of employment.

Staff and pupils should not bring in their own memory sticks to load data onto the School computer system. Any work pupils wish to present via a computer must be emailed to their teacher or uploaded onto their GDrive account via Google Classroom so it can be virus checked.

No software, whether licensed or not, may be installed on computers in the care of staff as the School does not own or control the licences for such software. As a School we subscribe to Spotify with no adverts and a shared user is available for staff to access.

Use of School systems

The provision of School email accounts, WiFi and internet access is for official School business, administration and education. There is also a guest WiFi available for guests and visitors. Staff and pupils should keep their personal, family and social lives separate from their School IT use and limit as far as possible any personal use of these accounts. Please be aware of the School's right to monitor and access web history and email use.

Inappropriate material

Accidental access to inappropriate materials must be immediately reported to the DSL. Deliberate access to inappropriate materials must be reported to a DSL and will be logged on the Online Safety Incident Reporting Form, which can be found as an appendix in the Online Safety Policy. This includes material generated by emerging technologies such as AI, where risks of deepfakes, misinformation, disinformation, conspiracy theories, or harmful synthetic content are present. Staff must report any exposure to such content, even if accidental, to the DSL immediately.

Depending on the seriousness of the offence, there will follow: an investigation by the Head, possible immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Use of personal devices or accounts and working remotely

All official School business of staff and Governors must be conducted on School systems, and it is not permissible to use personal email accounts for School business. All staff have access to OneDrive for storing and sharing school-related documents. Staff are advised to refrain from using personal email accounts for sending or receiving any school-related business.

Any use of personal devices for School purposes and any removal of personal data or confidential information from School systems – by any means, including email, printing, file transfer, cloud or (encrypted) memory stick – must be approved by the Senior Leadership Team. Should staff be required to work remotely, e.g., during the COVID-19 pandemic, then SLT will be deemed to have given permission for the removal of such data and information to the extent that it is necessary to continue to provide uninterrupted education services to our pupils.

Where permission is given for use of personal devices (for example for personal use in the staffroom), these must be subject to appropriate safeguards in line with the School's policies.

Remote access

Remote access to the School network is generally available via RDS.

Individuals are responsible for all activity via a remote access facility. This includes ensuring that they are logged out of all accounts after use, especially when accessing the network in shared or public spaces.

Monitoring and access

The School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education and the Prevent Duty. The School's web filtering and monitoring web service is Smoothwall.

Filtering and monitoring systems are reviewed at least annually by the DSL, IT Manager, governors and SLT to ensure they remain appropriate, effective and proportionate. The School will use the Department for Education's "Plan Technology for Your School" tool to support this review and ensure filtering and monitoring systems remain effective and proportionate. This review includes consideration of new technologies such as generative AI.

The School is constantly reviewing industry trends to improve the filtering and monitoring of internet use in accordance with Keeping Children Safe in Education and any other Department for Education and online safety statutory guidance.

Staff, parents and pupils should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose, including serious conduct or welfare concerns, extremism and the protection of others. As a school, aligned with the Online Safety Policy and Safeguarding and Child Protection Policy, we are able to filter web searches and have systems in place to help us track the usage of iPads and similar devices where specific users are not required to log in. The School requires all users of the wireless and local network to log in using their school-supplied credentials, with the exception of guest wireless users who use a code to connect with the external-only guest wireless system. The School monitors online activity.

All internet activity is monitored through the Smoothwall Firewall. A reporting system is in place for the IT Manager and Designated Safeguarding Lead (DSL) to monitor online activity and identify any areas of concern. It is the duty of the IT Manager to report any transgressions of the School's internet policy and/or use of obscene, racist, violent, extremist or threatening language detected by the system to the Head and DSL. Occasionally, it may be necessary for the IT Manager to investigate attempted access to blocked sites, and to do this, the IT Manager will need to set their internet access rights to 'unrestricted'. Whenever this happens, it should be recorded in the IT violations register and the Head notified.

Staff should be aware that all communications and online interactions must adhere to safeguarding principles to protect both staff and pupils and if they log on to a secure website (identifiable by https in the web address and a padlock symbol) from School IT equipment, their encrypted personal data will be inspected by the School's firewall, but remains secure.

Staff receiving suspicious emails containing attachments or links must not open them due to the risk of viruses, phishing, or ransomware. The IT Manager must be informed immediately if this happens accidentally. Regular training is given to help staff identify such scams.

The School is aware of its duty under Section 26 of the Counter-Terrorism and Security Act 2015 to prevent pupils from being drawn into terrorism (the 'Prevent Duty'). In accordance with the

Department for Education advice *Protecting children from radicalisation: the prevent duty* (2015) the School ensures that suitable filtering is in place, that the risk of online radicalisation is incorporated into the curriculum and that all teaching staff are aware of the risks posed by the online activity of extremist and terrorist groups.

Teaching precautions

Teaching staff should not use Google images searching while an interactive whiteboard or computer is in view of pupils; the board should be turned off.

Any educational material viewed on YouTube must be viewed beforehand by teaching staff and used through a YouTube filtering site (e.g., watchkin/safeshare) and/or another comparable site as recommended by the IT Manager.

If the internet is used in whole School assemblies and in class, then the material must be checked before viewing and any advertising/comments kept out of view of the audience.

When taking the register or performing similar tasks, staff should ensure that personal data is not visible on their screen or Interactive Whiteboard (IWB).

All staff should log off or lock the device that they are using before leaving it unattended. This applies particularly when devices are in shared spaces or classrooms.

Staff email etiquette

Users are responsible for all emails sent and for contacts made that may result in emails being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. Staff should respond within 24 hours to emails sent during the working week, where possible. Staff are not expected to respond to emails received after 18.00 unless they are of vital importance. Staff may, at their discretion, not respond to emails received during holidays/weekends until School resumes. Auto reply during school holidays is switched on for all teaching staff, which will inform senders that school is closed, and will provide a safeguarding email address.

Staff should not give pupils or parents and guardians their personal email addresses or reply to emails sent to their personal email addresses by pupils or parents and guardians.

Staff should not reply to individual emails that may have been sent to them by pupils; such emails should be forwarded to the Head.

Staff should not email School material to their personal email addresses. If they need to work on School material at home, they should access it from their School email address via OneDrive.

External storage devices are blocked from being used via a network policy. Please do not attempt to plug in any personal external device, as they will not respond.

Staff must avoid sending sensitive personal data via email unless encrypted or otherwise secured. The School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within the system, as well as deleted messages.

Personal use, personal devices, social media

Social networking sites such as Facebook should not be accessed from School computer equipment. Staff may use their personal devices to view such sites in the Staff Room.

Staff should be discreet when using their personal mobile devices in and around the School. Staff should not use their personal mobile devices when in class with pupils or in shared School areas (e.g., corridors, playground) during the course of the School day. Specific provisions for personal mobile devices apply to EYFS staff in accordance with the School's Safeguarding and Child Protection Policy.

Staff should not use their personal social networking sites to discuss confidential School matters or share pupils' work. Staff should not include parents or pupils as contacts on their social media sites.

Staff who use social network sites should have the highest level of privacy settings and ensure these are regularly updated. Social media platforms may change their privacy settings or policies over time. Staff should regularly review their privacy settings and ensure they are up to date with the latest platform changes. This helps maintain control over who can see their information and updates.

Staff should be aware that online behaviour, even outside of School hours and off-site, may be subject to scrutiny if it impacts pupil welfare, breaches safeguarding expectations, or brings the School into disrepute.

If a personal device is used to access the School email or network systems, the IT Manager must be notified immediately if this device is lost or stolen so that passwords to school accounts can be changed without delay.

Internet publishing statement

The School wishes for its website to reflect the ethos, diversity of activities, individuals and education that can be found at the School. However, the School recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the internet, staff should adhere to the following principles:

- Surnames of pupils must not be published
- No link should be made between an individual and any home address (including partial addresses or locations)
- Photos of pupils whose parents have opted out of publicly displaying their child's photograph should not be used on the School website, social media, newsletter or other publication. If photos are used, there should be no pupil name displayed
- Where there may be a child protection issue, no material should be published that could put the pupil at risk. In the case of a simple piece of artwork or writing, this may well be fine, but images should not be published. If in any doubt, refer to the School's Designated Safeguarding Lead

Retention of digital data

All members of the School community must be aware that all emails sent or received on School systems, including deleted emails, are retained indefinitely. Email accounts are closed when that person leaves the School, but the contents are retained indefinitely.

Emails and digital records will be retained in line with the School's Data Retention Schedule, ensuring compliance with the principles of UK GDPR and the Data (Use and Access) Act, which requires retention and searches to be reasonable and proportionate.

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School Privacy Notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. It is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way, no important information should ever be lost as a result of the School's email deletion protocol.

Pupil Google Classroom accounts are archived from 1st September each academic year. The entirety of the Google Classroom infrastructure is backed up weekly onsite. The IT Manager is able to reinstate accounts should access be required for safeguarding purposes.

Breach reporting

Data protection law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School, regardless of whether the personal data falls into a third party's hands. This would include:

- Loss of an unencrypted laptop or a physical file containing personal data
- Any external hacking of the School's systems, e.g. through the use of malware
- Application of the wrong privacy settings to online systems
- Misdirected post or email
- Failing to bcc recipients of a mass email
- Unsecure disposal

The School must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In line with the Data (Use and Access) Act, the School will adopt a "reasonable and proportionate" approach to investigating and responding to Subject Access Requests and personal data breaches, while maintaining a safeguarding-first approach. In addition, data controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. The School uses the GDPRiS platform to ensure compliance with this requirement.

If any member of the School community (including pupils where age appropriate) becomes aware of a suspected breach, they should notify the Bursar, who is responsible for data protection compliance within the School.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all members of the School community. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy, but failure to report a breach will be a disciplinary offence.

Loss of personal device

Under the unfortunate circumstances of your personal device, i.e., mobile phone, being lost or stolen, please contact the IT Manager as soon as possible so that your email account can be blocked or reset to prevent a potential data breach.

Breaches of this policy

Breaches of this Acceptable Use Policy and use of inappropriate language **by pupils** can be dealt with in a range of ways appropriate to the severity of the offence, including: removal of internet access rights; computer system access rights; meetings with parents or even exclusion. This is in accordance with School's Behaviour Policy.

Breaches of this Acceptable Use Policy **by employees** should be reported to the Head and will be dealt with according to the School's Capability and Disciplinary Policy and may, if the Head considers it appropriate, be reported to the police.

Breaches of this Acceptable Use Policy by contractors or service providers will result in immediate termination of contract and may, if the Head considers it necessary, be reported to the police.

Complaints

Complaints and/or issues relating to online safety should be made to the DSL.

Incidents should be logged on the Online Safety Incident Reporting Form, which can be found as an appendix in the Online Safety Policy, and the School procedure for investigating an online safety/e-safety incident should be followed.

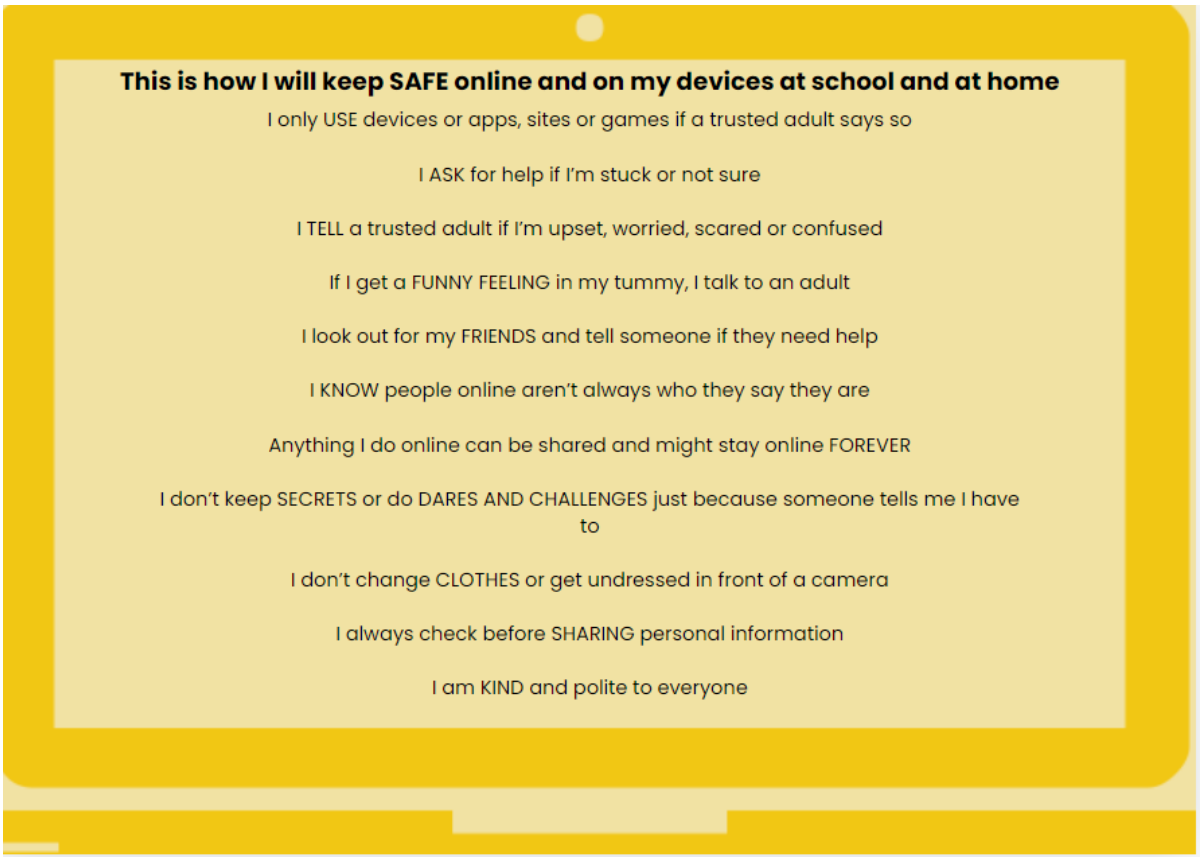
Linked policies

- Anti-bullying Policy for Pupils
- Anti-bullying & Harassment Policy for Staff
- Behaviour Policy
- Code of Conduct
- Code of Conduct for Other Adults
- Computer Studies Subject Policy
- Curriculum & Teaching and Learning Policy
- Online Safety Policy
- Prevent Policy
- Privacy Notice
- PSHE Policy
- Safeguarding and Child Protection Policy

- Social Media Policy
- Taking, Storing and Using Images of Pupils Policy

APPENDIX

Key Stage 1: Acceptable Use Agreement



Key Stage 2: Acceptable Use Agreement

I ask permission – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game. If I get a funny feeling, I talk about it.

I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

I learn online – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

I learn even when I can't go to school (e.g. covid isolation)– I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom when I am online. I don't expect teachers to behave differently online. If I get asked or told to do anything that I would find strange in school by anyone including a teacher, I will tell another teacher or ask my trusted adult to do so.

I am a good friend online and part of a community – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening I will tell my trusted adults.

I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I say no online if I need to – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

I am creative online – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.

I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.

I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult

I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

I follow age rules – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable.

I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

I respect people's work – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I must not share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

I know new online friends might not be who they say they are and I understand that it can be very unsafe to meet with friends I make online – I am careful when someone wants to be my friend online. I will check with a parent/carer before I arrange to meet an online friend and would never meet them without a trusted adult.

I don't do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

I keep my body to myself online – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

I am aware that my digital footprint is the record of all my interactions online – I know anything I do can be shared and might stay online forever.