



CHANNING SCHOOL

ONLINE SAFETY POLICY

This policy applies to the whole School including the EYFS

Updated	Review Date	Version
April 2024	April 2025	24.1

Reviewed by: Dan Grossman (Assistant Head Digital Technology), Joe Copson (IT Operations Manager), Jacqui Newman (Deputy Head Academic), Rachel McGinney (Deputy Head Academic of the Junior School)

Approved by: Freddie Meier (Deputy Head), Dina Hamalis (Head of the Junior School)

Signed by: Board of Governors

Online Safety Policy

This policy should be read in conjunction with the School's Safeguarding and Child Protection Policy and Procedures, Anti-Bullying Policy, PSHE and RSE Policy and the Staff Code of Conduct

Contents

Development and monitoring of the Policy

Scope of the Policy

Roles and Responsibilities

Policy Statements

The Education of Pupils

Education and Support of Parents / Carers

Education and training for Staff / Volunteers

Training for Governors

Technical – infrastructure / equipment, filtering and monitoring

Bring Your Own Device to Work Policy

Use of digital and video images

Data protection

Communications

Social Media - Protecting Professional Identity

User Actions - unsuitable / inappropriate activities

Responding to incidents of misuse, illegal incidents and other incidents (flowchart)

School actions and sanctions

Appendices

Appendix A - Pupil Digital Technology Acceptable Use Policy

Appendix B - Pupil iPad Acceptable Use Policy

Appendix C - Pupil Chromebook Acceptable Use Policy

Appendix D - Pupil Artificial Intelligence Acceptable Use Policy

Appendix E - Pupil Digital Technology Acceptable Use Agreement

Appendix F - e-Safety rules for our EY/KS1 and KS2 pupils

“At Channing we foster intelligent, creative users of technology who are ready for what happens next”

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Development and monitoring of the Policy

This policy has been developed by the Digital Strategy Group made up of:

- Director of Digital Learning and Technology / Online Safety Officer
- Bursar
- Deputy Head Academic (Senior School)
- Deputy Head Academic (Junior School)
- Junior School Computing Coordinator
- IT Operations Manager

The committee also consults other members of staff in particular the Head of PSHE in the Senior School and the PSHE Coordinator in the Junior School. Consultation with the whole school community takes place through a range of formal and informal meetings.

The committee oversees and monitors the implementation of this policy.

The committee monitors the impact of this policy using logs of internet activity (including sites visited), internal monitoring data for network activity, and surveys / questionnaires from pupils, parents and staff.

The Governing Body receives a report on the implementation of this policy annually in November as part of the safeguarding report. The report is generated by the committee and includes anonymous details of online safety incidents.

Should a safeguarding concern arise, the committee follows the procedures laid out in the School's Safeguarding and Child Protection Policy.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of the School ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the School, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the School's published Behaviour and Discipline Policy.

The School will deal with such incidents using this policy, behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of School.

Roles and Responsibilities

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

The following section outlines the online safety roles and responsibilities of individuals and groups within the School:

Board of Governors

Governors are responsible for signing of all policies and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring relevant reports. The safeguarding governor will receive any reports of online concerns from the Deputy Head in his role as Designated Safeguarding Lead and may request to see Incident Logs or to discuss online Safety issues directly with the Online Safety Officer who is the Director of Digital Learning and Technology.

Headmistress and DSLs

- The Headmistress has a duty of care for ensuring the safety (including online safety) of members of the School. The day to day responsibility for online safety will be delegated to the DSLs.
- The Headmistress and the DSLs should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headmistress and DSLs are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headmistress and DSLs will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.
- The Headmistress and DSLs will receive regular monitoring reports from the Digital Strategy Group.

Online Safety Officer

- Takes day to day responsibility for online issues and has a leading role in establishing and reviewing the School's Online Safety Policy and documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- Provides training and advice for staff;
- Liaises with the Local Authority as required;
- Liaises with the Bursar and technical staff as required;
- Receives reports of online safety incidents and creates a log of online safety incidents;
- Reports any issues to the DSLs;
- Reports regularly to the Senior Leadership Team.

Bursar and IT Operations Manager

The Bursar is supported by the IT Operations Manager who is responsible for ensuring

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the School meets required online technical requirements and any National or sector specific guidance that may apply;

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- a filtering system is applied and updated on a regular basis and that its implementation is delegated to appropriate members of staff;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of all school ICT systems are regularly monitored;
- that the software systems are monitored and updated as required.

Teaching and Support Staff are responsible for ensuring that

- they have an up to date awareness of online safety matters and of the current School policies;
- they have read and understood the School policies, including the Staff Code of Conduct;
- they report any suspected misuse or problem to the Digital Strategy Group;
- all digital communications with other staff, pupils and parents should be on a professional level and only carried out using official school systems;
- online safety is embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the online safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- 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.

DSLs

Should be trained in online safety issues and be aware of the potential for serious Safeguarding and Child Protection / safeguarding issues that may arise from

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate online contact with adults / strangers;
- potential or actual incidents of grooming and sexting;
- cyber-bullying;
- any other Safeguarding and Child Protection concerns listed in Annex B of KCSiE, including Child Sexual Exploitation (CSE) and the Prevent Duty.

Digital Strategy Group (DSG)

The DSG provides a consultative group that has wide representation from the School with responsibility for issues regarding online safety including drafting and monitoring the Online Safety Policy and associated documents.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Members of the DSG will assist the Online Safety Officer with

- the production / review / monitoring of the School's Online Safety Policy and associated documents;
- guidance on content filtering;
- reviewing the online safety curricular provision – ensuring relevance, breadth and progression;
- advice on monitoring the network and specifically internet use;
- consulting stakeholders – including parents and pupils about the online safety provision.

Pupils

- are responsible for using the school systems in accordance with the Pupil Digital Technology Acceptable Use Policy (Appendix B);
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand the policy on the use of mobile devices and digital cameras as per the Agreement. They should also know and understand policies on the taking / use of images and on cyber-bullying as set out in the School's Anti-Bullying Policy;
- should 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.

Parents / Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the School website, the VLE and the National Online Safety Platform and app as appropriate. The School will take every opportunity to ensure that parents and carers are aware of what their children are being asked to do online, including the sites they will be asked to access.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website / VLE and online pupil records;
- their child's personal devices in the School.

Policy Statements

Education of Pupils

Whilst regulation of ICT use 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 is therefore an

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing and PSHE and should be regularly revisited and monitored by the Deputy Head Academic;
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that 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;
- Where pupils are encouraged to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Operations Manager 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.

Education and support of Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, the school website, the school VLE, School Base;
- Parents / Carers evenings sessions;
- High profile events and campaigns eg Safer Internet Day, Wellbeing Week.

Education and Training for Staff / Volunteers

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. It is expected that some staff will identify online safety as a training need within the appraisal process.
- All new staff should receive online safety training as part of their induction programme, including the School's expectations, roles and responsibilities in relation to filtering and monitoring ensuring that they fully understand the School's Online Safety policy and associated elements in the School Policies folder.
- The Online Safety Officer will receive regular updates through attendance at external training events.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and during INSET days.
- The Online Safety Officer will provide advice / guidance / training to individuals as required.

Training for Governors

Governors should be briefed on the initiatives being adopted by the School to support online safety and as part of the regular updates on Safeguarding will also be briefed on any online safety issues.

All governors receive appropriate safeguarding and child protection (including online) training at induction.

Technical – infrastructure / equipment, filtering and monitoring

The School will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

The IT Department holds numerous protocols on network security, filtering systems, back-up, etc. The general principles applied are as follows:

- School technical systems will be managed in ways to ensure that the School meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of the School technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users will be provided with a username and secure password by the IT Operations manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and passwords;
- The “administrator” passwords for the school ICT system, used by the IT Operations Manager (or other person) must also be available to the Bursar and to Toucan Computing. They should be kept in a sealed envelope in the School safe;

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- The IT Operations Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations;
- Internet access is filtered for all users;
- The School has provided differentiated user-level filtering for staff via a dedicated wi-fi network which is not accessible by pupils;
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement for Pupils and Staff Code of Conduct;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The School infrastructure and individual workstations are protected by up to date virus software.

Bring your Own Device to Work Policy

We recognise that many of our staff have personal mobile devices (such as tablets, smartphones and handheld computers), which they could use for work purposes, and that there can be benefits for both us and staff, including increased flexibility in our working practices, in permitting such use. However, the use of personal mobile devices for work purposes gives rise to increased risk in terms of the security of our IT resources and communication systems, the protection of confidential and proprietary information, and compliance with legal obligations.

Please refer to the section *Use of personal mobile devices by staff* (p. 10) of this policy for more information.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 e.g. on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the taking, sharing, distribution and publication of those

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Staff, pupils and parents should refer to the Photography Policy in the Safeguarding and Child Protection Policy and Procedures for more detailed information.

- 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' first names and initials can be used in school publications.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and used for other marketing purposes by the school. Permission slips are generally signed prior to a pupil joining the school. The School retains a record of pupils whose parents have not provided permission for their photographs to be used. In some circumstances it may also be appropriate to seek permission from pupils prior to using images in school material.
- Pupil's work can only be published with the permission of the pupil and the parents or carers.

Pupils should also see the Pupil's Digital Technology Acceptable Use Policy (Appendix A) for more information.

Data Protection

The School has a comprehensive Data Protection Policy which covers personal data which is recorded, processed, transferred or made available by the School. The School is registered with the Information Commissioner and all data is processed according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Staff are advised to acquaint themselves with the School's Data Protection Policy and to exercise care whenever using data held by the School.

Use of personal mobile devices by pupils

In the Junior School, Key Stage 2 pupils in Year 5 and 6, who walk home independently, can bring mobile phones to school. These phones, along with any other personal devices, must be handed to the Office at the start of each day (immediately upon arrival) and must remain there for the duration of the day. Pupils will then collect their mobile phone, fitbit, or smart watch device when leaving school (this could be after normal collection, after Mini Owls, Clubs or Late Owls). Parental permission for having a phone at school and walking home is found on SchoolBase (under Consents).

In the Senior School, pupils are allowed to bring their personal mobile devices to school with them, but we operate the following policy:

- For pupils in Years 7-10, the devices must be turned off and locked in a Yondr pouch upon entry to the school site. The devices must remain off and in the Yondr pouch for the duration of their time on site (or on school trips as decided by the lead teacher). The pouches must only be unlocked at the end of the school day or when the pupils are leaving the school site for the last time.
- For pupils in Year 11, the devices must be turned off and kept in a bag or locker out of sight. Devices are confiscated from Year 11 pupils who have them out or are using them during the school day. Confiscated devices are passed to the Deputy Head from whom pupils must collect their phones at the end of the school day or when the pupils are leaving the school site for the last time.
- For pupils in Year 12 and 13, the devices must only be used within the confines of the Sixth Form Centre. Devices are confiscated from Year 12 and 13 pupils who have them out or are using them anywhere else during the school day. Confiscated devices are passed to the Deputy Head from whom pupils must collect their phones at the end of the school day or when the pupils are leaving the school site for the last time.

Use of personal mobile devices or any device with taking and sharing capabilities by staff

In order to promote the school's approach to a phone-free environment, staff are asked to only use their personal mobile devices in designated staff work / dining / recreational areas. Staff should not use their personal mobile devices when moving around the school where they are visible to pupils. Staff should not use personal mobile devices in lessons other than as verification for 2FA.

In the Junior School, personal mobile devices are forbidden in the EYFS (Reception classrooms or where there are Reception children, e.g. in the playground). Staff must also ensure that personal mobile phones are out of sight in Late Owls and that they are not interacting with pupils.

The School has a number of policies which support the use of technology at school which are set out in the School Policies folder. Some general principles consistent with these policies are outlined below:

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE, etc.) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications except in exceptional circumstances.
- Whole class / group email addresses may be used at KS1 and 2, while pupils at KS3 and above and all staff and governors will be provided with individual school email addresses for educational use.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes the School has a comprehensive policy that sets out clear guidance for staff to manage risk and behaviour online.

The School recognises that it has a duty of care to provide a safe learning environment for pupils and staff. The School could also be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. The School considers it has taken reasonable steps in its policy to prevent predictable harm and provide sensible guidance to staff.

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through limiting access to personal information:

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- Training to include: acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk where appropriate.

The School's use of social media for professional purposes will be checked regularly by the Online Safety Officer and Bursar to ensure compliance with the School's policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The School policy restricts usage as follows:

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
------------	-----------------------------	--------------------------------	--------------	--------------------------

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of					X

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

or comments that contain or relate to:	sexual orientation) - contrary to the Public Order Act 1986					
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
online gaming (educational)		X				
online gaming (non educational)	X					
online gambling				X		

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

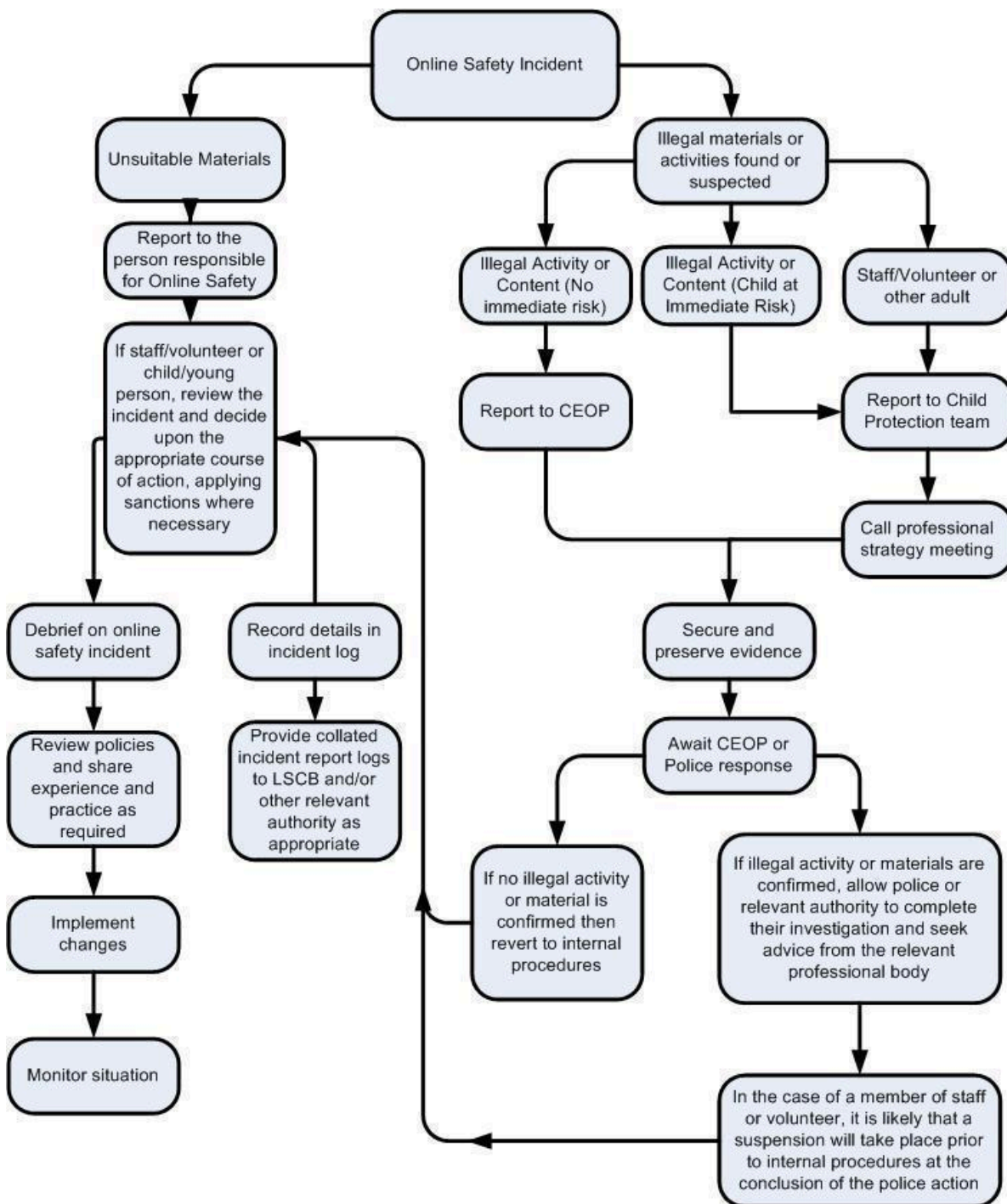
online shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Responding to incidents of misuse, illegal incidents and other incidents (flowchart)

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

It is hoped that all members at Channing will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff or Governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer (or mobile device) that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of ‘grooming’ behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
 - any material associated with radicalisation or which might be considered as part of the Prevent Programme.
- Isolate the computer (or mobile device) in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

The School will deal with incidents that involve inappropriate rather than illegal misuse in a proportionate manner and consistent with the school’s existing disciplinary procedures.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Appendix A - Pupil Digital Technology Acceptable Use Policy

1. Digital Technology in the Curriculum

Digital and online resources are used extensively across the curriculum at Channing. Pupils are required to sign a Digital Technology Acceptable Use Agreement that acknowledges this document's contents.

2. General Conduct

It is essential for guidance to be given on how these technologies are to be used appropriately on a regular and meaningful basis. As part of preparing pupils to ensure the appropriate use of online and digital resources the school has a framework for teaching online skills within a range of curriculum areas, notably in Computing lessons, the PSHE programme, assemblies and peer to peer briefings.

This policy supports, and should be read in conjunction with, the school's Anti-Bullying Policy and the Anti-Cyberbullying Code.

3. Managing the Internet

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity. Filters are in place to prevent access to inappropriate websites.
- The school is also able to monitor and oversee all usage of the internet by pupils when in school and using the school network. The school is not able to monitor internet usage by pupils using their own mobile devices with private access to a 3G or 4G network which are not permitted in school with the exception of the Sixth Form.
- Pupils will be advised on the most appropriate websites and resources to use for research and data collection. Staff should preview any recommended sites before use.
- If web-based research is set for homework, specific sites might be suggested that have previously been checked by the teacher, but pupils will also be encouraged to conduct independent research.
- Pupils should only access websites and resources they know to be appropriate. If they are unsure, they should exercise caution and check with their teachers before accessing websites or resources.

4. Use of Images and Film

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- With the written consent of parents (on behalf of pupils), the school permits the appropriate taking of images by staff of pupils for use by the school.
- Staff should inform pupils before images are taken as in some instances pupils may wish to withdraw permission for images to be taken.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record audio or visual images of pupils, staff and others without advance permission from those being recorded, photographed or filmed, and the permission of a teacher.
- Pupils must have permission from a teacher before any image taken at school can be uploaded for publication. This permission will generally be refused given that consent may be required from all individuals who feature in the image.

5. Personal Mobile Devices

- At the Junior School mobile devices belonging to Y5 and Y6 pupils are to be handed in at the beginning of the day and are handed back at the end of the day.
- At the Senior School, the following rules apply to mobile devices:
 - for Years 7-10, personal mobile devices must be kept in a sealed Yondr pouch upon entering school, and should only be removed when leaving school at the end of the school day
 - for Year 11, personal mobile devices are to be switched off and must not be seen or heard whilst on site
 - For Years 12-13, personal mobile devices may only be used in the Sixth Form Centre
- The school is not responsible for the loss, damage or theft of any personal mobile devices.
- It is not appropriate for pupils' personal devices to be used to make images or sound recordings as all pupils are provided with a school iPad or chromebook which should be used for this purpose.
- Any personal devices used at school must not have any inappropriate or illegal content on the device.
- Personal devices will not be allowed access to the school network. Exceptions are made for members of the Sixth Form who use their own approved devices, and only on the

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Kaffeehaus network. In order to gain access, pupils must log in upon joining Year 12 using their school-assigned username and password.

- No personal mobile devices are allowed in any public examination. Additionally for tests or other assessed activities, pupils may be required to hand in any personal device which is in their possession including smart watches, smart pens, data readers and fitness trackers for the duration of the test or assessed activity.
- Inappropriate or improper use of mobile devices at school, especially in situations which might compromise the academic integrity of a lesson or other teaching activity, or the Channing Code of Conduct, may result in devices being confiscated.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

6. School iPads and chromebooks

- Channing Junior School pupils have access to shared chromebooks and iPads, which are stored in lockable cabinets. Years 5 and 6 are allocated a chromebook each, for the year, but they are left onsite and never taken home.
- Channing School provides iPads to all pupils in the Senior School. iPads are not provided to pupils joining in Year 12, nor are they replaced for pupils in the Sixth Form.
- Channing School provides chromebooks to all pupils in the Senior School in Year 10 and 11. Chromebooks are not provided to pupils joining in Year 12, nor are they replaced for pupils in the Sixth Form.
- All school devices are managed through device management software which enables the school to monitor which applications are being used on the devices.
- Whilst the devices are purchased by parents, the school reserves the right to confiscate any device provided by the school to ensure that it is being used appropriately.
- Devices provided by the school will only be able to access the internet in school via the school's secure wi-fi network which is monitored.
- Pupils in Year 7 (and those joining) in Year 8 and 9 are given training in setting up their iPads and how to store files when the iPads are given to the pupils.
- Pupils in Year 10 (and those joining in Year 11) are given training in using their chromebooks when the chromebooks are given to the pupils.
- Pupils must sign the appropriate use agreement (**see Appendices a and b**) on being issued a school iPad / chromebook and use will be reviewed on a termly basis.
- Use of iPads and chromebooks is subject to the School's Discipline and Behaviour policy and code of conduct, as well as this Pupil Digital Technology Acceptable Use Policy.
- iPads and chromebooks remain school property until final payment is made to the school. iPads and chromebooks are provided to pupils for educational use only.
- In cases of inappropriate use, the pupil will face disciplinary sanctions and the school reserves the right to request that the iPad or chromebook be returned to the school.
- iPads and chromebooks are insured from damage whilst in school and are the responsibility of the pupils at all times.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- The IT Support Team must be notified of any damaged iPad or chromebook that needs replacing. In most instances, other than negligence, the school will be able to replace the device with no charge. No non-school devices will be allowed on the school network.
- iPads and chromebooks must be returned to Channing whenever the school requests - this will happen from time to time for security and upgrade purposes.
- It is the pupil's responsibility to bring the iPad or chromebook to school each day fully charged, in working order and named clearly.

7. Social Media

- Pupils are not permitted to access their social media accounts on any device whilst at school.
- Pupils in Years 7-11 will not be able to upload blocked social media apps to their school iPads.
- Any use of social media should conform to the school's Anti-Cyberbullying code and the Pupil Online Safety Protocol.
- Pupils should not seek to 'befriend' any member of staff.
- Pupils are asked to report any incidents of cyberbullying to their Head of Year or the Deputy Headteacher.
- Pupils may only create blogs, wikis or other online areas at school in order to share and present their work with other pupils with express permission from the relevant teacher.

8. Firefly / Google Classroom / other VLEs

Firefly and Google Classroom are Virtual Learning Environments (VLEs) which provide a dynamic learning space for enhancing the curriculum through collaboration, personalisation, interactive content, assessment and real-time feedback. The use of Firefly, Google Classroom, or any replacement VLE is subject to Channing's internet and network use policies.

When using Firefly, Google Classroom, or any other VLE provided, pupils should:

- Log in and out carefully using only their given network identity.
- Identify themselves honestly to other users online.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- Respect other people's views and beliefs.
- Post comments appropriate to the particular discussion.
- Enjoy the interaction with fellow pupils and their teachers in a friendly and intellectually stimulating environment.
- Report any abuse or problem immediately.

When using Firefly, Google Classroom, or any other VLE provided, pupils should not:

- Post anything illegal, obscene or offensive.
- Log in with any username other than their own.
- Copy or forward e-mail, messages, images or files without permission.
- Use storage facilities for inappropriate or non-educational material.
- Behave in an impolite manner.
- Further detail on the appropriate use of Firefly, Google Classroom, or any other VLE provided during periods of virtual schooling is provided in the Virtual School Policy.

9. Artificial Intelligence

The school recognises the rapid advancements and growing presence of artificial intelligence (AI) technology in today's world. To harness the potential of AI in education while ensuring safe and responsible use, **Appendix c** outlines guidelines for pupils' engagement with AI technology. For the purposes of this policy, the term AI refers to generative AI technologies; these are technologies that are able to use machine learning to generate entirely new content such as text, images, audio and other media.

This policy emphasises the importance of appropriate use of AI by preserving academic integrity, ensuring accurate referencing and citation, upholding ethical standards, and maintaining data privacy. By adhering to these principles, pupils will be equipped to navigate the realm of AI technology in a responsible and beneficial manner, fostering a positive and inclusive learning environment.

10. Incident Reporting, Misuse, and Inappropriate Material

- Pupils are aware of the procedures for reporting accidental access to inappropriate materials.
- Pupils are made aware that any breach must be immediately reported to a member of staff.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- Deliberate access to inappropriate materials by any pupil will lead to an investigation by the Headteacher and could possibly lead to a permanent exclusion and involvement of police for very serious offences.

This Pupil Digital Technology Acceptable Use Policy must be read alongside the school's safeguarding and child protection policy. All use of digital technology in the school must be cognisant of these policies, which are available on the School Website.

Violation of any part of this school policy may result in further actions, including but not limited to academic penalties, loss of privileges, counselling and parental involvement. The school administration reserves the right to modify or update this policy as necessary to ensure the safe and responsible use of digital technology in the educational environment.

The Director of Digital Learning and Technology is responsible for this policy, and for reviewing its content.

Appendix B - Pupil iPad Acceptable Use Policy (Y7-11)

'iPad' refers to the 'school iPad' issued by Channing School. Pupils are not allowed to use any other iPad or mobile device in school unless agreed by the school.

A set of apps will automatically be installed at the time of setting up. The following apps are blocked for Years 7-11:

- Social media apps such as Instagram, Whatsapp and Snapchat
- Film and TV streaming apps such as Netflix

In addition, the following functions are blocked:

- iMessage
- FaceTime
- App Store

In the classroom

iPads are only to be used in class for activities directly related to the lesson with the teacher's permission. iPads should remain in a pupil's bag until instructed to remove it by the teacher. iPads should thereafter be placed face down on the desk when not in use. iPads should be locked in lockers when not in use and lockers must be padlocked. All pupils in Years 7-9 using iPads as part of their lesson must be a member of their teacher's Apple Classroom, and must give full access to their teacher including the ability to view and lock their screen.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

During break and lunch time

Pupils in Years 7-9 are not permitted to use their iPads during break or lunchtime, in any part of the school or for any reason, with the following exceptions:

- pupils working on their iPads in the Library
- pupils using their iPads as part of a supervised and authorised extra-curricular activity

Appropriate use

No taking or use of photos / video / recording is allowed without the subject's permission, and a teacher's permission.

No material should be published through any media outside of the school environment *without specific permission from a teacher*.

Within the school day, communication with other pupils via text / e-mail / chat or any other media is not permitted *without specific permission from a teacher*.

Pupils may be asked to show the iPad's content and applications to teachers at any time.

Appendix C - Pupil Chromebook Acceptable Use (Y10-11)

'Chromebook' refers to the 'school chromebook' issued by Channing School. Pupils in Years 10 and 11 are not allowed to use any other chromebook or laptop device in school unless agreed by the school.

In the classroom

Chromebooks are only to be used in class for activities directly related to the lesson with the teacher's permission. Chromebooks should remain in a pupil's bag until instructed to remove it by the teacher. Chromebooks should thereafter be on the desk with the screen closed when not in use. Chromebooks should be locked in lockers when not in use and lockers must be padlocked. In the Junior School, shared chromebooks are stored in lockable cabinets.

Appropriate use

No taking or use of photos / video / recording is allowed without the subject's permission, and a teacher's permission.

No material should be published through any media outside of the school environment *without specific permission from a teacher*.

Within the school day, communication with other pupils via text / email / chat or any other media is not permitted *without specific permission from a teacher*.

Pupils may be asked to show the chromebook's content and applications to teachers at any time.

Appendix D - Pupil Artificial Intelligence Acceptable Use (all pupils)

General Guidance

- Pupils may use AI technology for educational purposes, including research, problem-solving, resource-creation and enhancing their learning.
- Pupils may also use AI technology in a creative, non-educational capacity, provided this usage meets all other criteria of safe and acceptable use.
- Pupils must always use AI technology in an ethical and responsible manner, respecting the rights and dignity of others, and adhering to the principles of the Digital Technology Acceptable Use Agreement and the Channing e-Promise.
- Pupils should only use AI technology that is age-appropriate and aligned with the educational goals set by the school.

Academic Integrity

- Pupils should use AI technology to support their learning and academic growth, but they must not rely on AI to complete assignments or assessments that require independent thinking and original work.
- Pupils should only use AI technology to produce or contribute to pieces of submitted work when explicitly permitted to do so by their teacher.
- Pupils must inform their teacher when they have used AI technology to produce or contribute to any permitted piece of work, with an outline of the involvement of the AI technology.
- Pupils must not use AI technology to plagiarise others' work and pass it off as their own, or infringe upon intellectual property rights.
- Pupils must not use AI technology to produce all or part of any controlled assessments that contribute to an overall qualification, including but not limited to NEAs, EPQs and other coursework.

Referencing and Citation

- Pupils are responsible for providing accurate references and citations for any AI tools, algorithms or models they use in their academic work.
- When using AI-generated content, pupils must clearly indicate the involvement of AI in the creation process.

Ethical Considerations

- Pupils must not use AI technology for malicious purposes, such as hacking, cheating or spreading misinformation.

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

- Pupils are encouraged to consider the potential societal impacts of AI technology and engage in discussions on ethics and responsible AI use.

Data Privacy

- Pupils must respect data privacy and adhere to applicable laws and regulations.
- When using AI technology, pupils must only collect, store, and use data that is necessary for the intended educational purpose.
- When using AI technology, pupils must not share their personal data or that of anyone associated with the school.
- Pupils must seek appropriate permissions and consents when dealing with personal or sensitive data.

Appendix E - Pupil Digital Technology Acceptable Use Agreement

I confirm that I have read and understood the following acceptable use protocols:

- Channing School Pupil Digital Technology Acceptable Use Protocol
- Channing School Pupil iPad Acceptable Use Protocol
- Channing School Pupil Chromebook Acceptable Use Protocol (Y10 only)

By signing this form, I understand that:

- the school will monitor my use of the systems, devices and digital communications
- the school systems and devices are intended solely for educational use and that I will not use them for personal or recreational use
- I must act as I expect others to act toward me
- the school has the right to take action against me if I am involved in incidents of inappropriate behaviour relating to digital technology

I also understand that the above applies to:

- using the school systems and devices (both in and out of school)
- using my own devices in the school (when allowed)
- using my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school e-mail, VLE, website etc.

 Name:

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

Form:

Signed:


Date:

If you do not sign and return this agreement, access will not be granted to school systems and devices.

The Director of Digital Learning and Technology is responsible for this agreement, and for reviewing its content.

Appendix F - e-Safety rules for our EY/KS1 and KS2 pupils

EY/KS1



Only go online when there is a grownup nearby.

When you start working, set a timer so that you know when to stop.


Don't share any personal information online.

Don't click on anything that you are unsure about.

Seesaw and Firefly are only to be used to complete work set by your teacher.

Only share positive, kind comments when you are online.

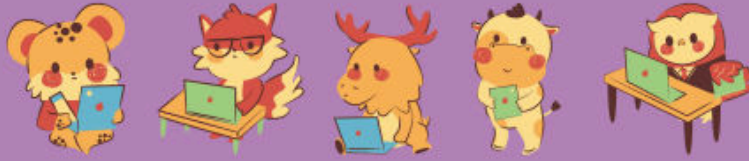
Tell a grown up if anything makes you feel worried.



CHANNING

The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.

KS2



Use classroom language

There are lots of phrases/abbreviations that you might use when you are talking to your friends such as LOL, but these shouldn't be used when you are using the school platforms.

Take regular screen breaks

It is really important to take a break from looking at your screen every 20 minutes to give your eyes a rest.

Always conduct video learning in an open space at home

If possible, try to complete your online work in a space where your parents/carers can see what you are looking at. It will help them to be aware of the things you are learning and keep you safe.

Only communicate through approved school portals and platforms

You should only be using Firefly, Seesaw or Google Classroom to communicate with your teachers/friends about your learning.

Don't share passwords or other sensitive information

To stop other people accessing your account and keep you safe, please make sure that you never share your password with anyone else.

Don't use school platforms to discuss personal matters

Remember that the comments that you post online should always relate to your work - no other issues should be discussed.

Only share positive/supportive comments with your peers

It is really helpful to share positive comments about the work of your classmates as well as tips to help them to improve but these must always be supportive to help us to grow.

Look after your mental health and well being

While working on a device can feel fun, if you are finding the work challenging, remember to talk to the nearest adult as they will be able to support you.

If you are concerned or have any questions, please speak to the nearest adult at home or school.



The Digital Strategy Group monitors this policy regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. It is reviewed at least annually.