Corsham Primary School

Acceptable Use & E-Safety Policy (Internet)

Reviewed: December 2021

Policy Ratified by the LGC: January 2022

Next Review Date: December 2022

Corsham Primary School

Acceptable Use & E-Safety Policy (Internet)

This Acceptable Use Policy should be read in conjunction with Corsham Primary School's Safeguarding, Confidentiality, Computing and ICT, Secure Data Handling, Data Security Document Marking, Behaviour and Anti-bullying policies.

What does an 'Acceptable Use & E-Safety Policy' cover?

This policy addresses all rights, privileges and responsibilities associated with the Internet. Examples include: websites, email, chat, Virtual Learning Environment, video, discussion group's bulletin boards, real-time conferencing, and social networking sites.

Rationale

The Internet has become an important aspect of everyday life to which children need to be able to respond safely and responsibly.

At Corsham Primary School we believe that the Internet offers a valuable resource for teachers and children providing ways to communicate with others world-wide and initiate cultural exchanges between pupils. Access to the Internet offers both children and teachers vast, diverse, and unique resources and helps to raise educational standards. It supports the professional work of staff as well as enhancing the school's management information and business administrative systems.

The main reason that we provide Internet access to our teachers and students is to promote educational excellence by facilitating resource sharing, innovation, and communication. Access to online interactive learning spaces where pupils can access targeted learning and where they can publish their own learning, such as our Virtual Learning Environment, Immersive Space and Pod are hugely beneficial to children, and encourage them to extend their learning beyond the classroom. However, for both students and teachers, Internet access at school is a privilege and not an entitlement.

Although we use the latest and most advanced filtering systems at Corsham Primary School, there is always a small risk inherent with Internet use that children may encounter inappropriate material on the Internet. The school will actively take all reasonable precautions to restrict pupil access to both undesirable and illegal material, as well as educate pupils to take appropriate action if they do come across such material. This policy sets out measures to be taken that minimise these risks. It is recognised that this policy cannot cover all eventualities: there may be times where professional judgement is required to deal with issues not covered in this document. In these situations, staff will advise the Head of School of the justification for these actions.

This document applies to all members of staff and pupils at Corsham Primary School, including senior leaders, teachers, support staff, governors and volunteers. Staff should review their practice in terms of the continually changing world of social networking and internet-based software, and ensure they follow the guidance in this document.

Aim

To ensure that children and adults can use the Internet safely and responsibly as an integral part of planning, delivering and resourcing lessons in all subjects of the curriculum, both within and outside school hours.

Guidelines

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils who use it responsibly.

  - In Foundation Stage nearly all of access to the Internet will be through adult demonstration. However, there may be situations when children have supervised access to specific teacher approved on-line materials.

  - At Key Stage 1 the majority of access to the Internet will also be through adult demonstration. However, there may be situations when children have supervised access to specific teacher approved on-line materials.

  - At Key Stage 2 Internet access will be granted to a whole class as part of a scheme of work, after discussion on responsible Internet use. This will involve the use of recommended search engines. The search engine www.ecosia.org is recommended by the school – Ecosia is accessed through a proxy set up by our technician company, Oakford – this proxy enforces the safest settings online so pupils cannot change them.

- Children and staff (teaching and non-teaching) must never knowingly seek to view material over the Internet that is illegal, pornographic, exploitative to children, violent, sexist, racist, or in any other way offensive or unsuitable within a school environment.

- The school subscribes to a filtered Internet service South West Grid for Learning (SWGFL) for the Broadwood site and School's Broadband (supported by Soft Egg) at Pound Pill. This service ensures that access to inappropriate sites is blocked; the content of web pages or searches is dynamically filtered for unsuitable words; web browsers are set to reject inappropriate sites and logs are made of banned internet sites visited by pupils and students. The Lead Computing Engineers will make regular checks in liaison with our technical support company, Oakford, School's Broadband and SWGfL to ensure that the filtering system selected is effective in practice. The school can elect to ban individual websites or search words that it considers inappropriate on top of the SWGFL and School's Broadband level of filtering. All staff are trained to identify any inappropriate websites and can contact

the company directly (School's Broadband at Pound Pill and SWGFL at Broadwood) so that they can be added to the filtered list.

- All children will be taught about the acceptable and responsible use of the Internet (e-safety lessons are planned into both the Computing and the PSHEE curriculum and are taught at least once a year in conjunction with Safer Internet Day) and what to do if they come across inappropriate material - the expectation is that they will minimise the application window and inform an adult immediately if they encounter any material that makes them feel uncomfortable. The adult must then report this to a member of staff who will contact SoftEgg (Pound Pill site) or SWGFL (Broadwood site) directly who will filter the website.

- As well as teaching children about e-safety through Computing or PSHEE lessons, we also promote safe internet usage across the school with e-safety displays and posters.

- A responsible adult will closely monitor and supervise use of the Internet at all times and inform the Lead Computing Engineers in the unlikely situation that any inappropriate material is seen - if unsuitable sites are discovered the address and content will be reported to the Lead Computing Engineers who will then inform 'SWGFL' or/and SoftEgg of the inappropriate material and / or add them to the filtered list.

- Each class teacher will put sanctions in place (at an appropriate level whilst adhering to the School's Behaviour Policy) for children who contravene the provisions of this policy – if children repeatedly break the rules, a meeting will be called with the parents.

- Parents receive an e-safety document on a yearly basis, linked to Safer Internet Day, informing them of websites to visit to find out more information regarding helping their children stay safe online.

    - Access in school to external, web-based, personal e-mail accounts is denied for network security reasons, although school email accounts are set up on teacher iPads.

    - It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender.

- Whilst in school, children do not have access to public or un-moderated chat-rooms – only regulated educational online discussions or forums (such as commenting on Seesaw) will be permitted.

- Pupils do not use mobile phones during lessons or formal school time (unless for medical reasons) – any mobile phones brought to school must be handed in to the Class Teacher. It is forbidden to send abusive or otherwise inappropriate

messages using the facilities provided by the school network or using personal devices of any kind.

- The school's computer network security systems are reviewed regularly and all user files, temporary Internet files and history files will be monitored by our technical support company, Oakford.

- Virus protection software is installed and updated regularly by Oakford
- Data on the school server is backed up remotely by Oakford.

- All access to the school network requires entry of a recognised User ID – pupils and staff must log out after every network session.

- Pupils and staff must NOT: upload or download non-approved application software; use any form of personal storage devices (USB memory sticks, hard drives, etc.) on the school network without specific teacher permission and a virus check or break copyright and intellectual property rights rules.

- Staff must ensure that the pages of any personal social networking sites (e.g. Facebook / Instagram / Twitter / YouTube / TikTok, Twitch, etc.) they are a member of are of an appropriate nature and that the pages of any 'friends' that they are linked to are also appropriate. Comments posted on social networking sites must not in any way denigrate the school, staff or pupils of the school. General comments about work are acceptable, but negative comments or negative references to specific members of staff, pupils, parents or governors are not. The advice of this policy is not to comment about the school, work or people associated with the school at all. If inappropriate comments are seen, staff have an obligation to follow the school's Whistle-blowing policy and report this to the Senior Management Team and/or Lead Computing Engineers. Staff must NOT agree to become 'friends' with or 'follow' any pupil currently at Corsham Primary School – should they be asked they should decline, and then discuss the reasons why not with their class in a circle time. Staff must not access personal social networking sites on their school computer whilst on school premises. Staff personal social networking sites' accounts such as Facebook, Instagram, YouTube, TikTok, Twitch may be accessed but only outside of the school network, i.e. accessing home wireless systems; Content may not be downloaded from these sites onto or using school equipment.

- Staff and pupils should consider carefully the implication of what they publish to social media, such as video sharing sites, e.g. YouTube, and blogging sites, e.g. Twitter, both in a personal and school capacity. Staff should ensure that their conduct befits their professional role in school. All adults working at Corsham Primary School have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. Staff, particularly in the case of new staff, should review their social networking site content to ensure that

information publicly viewable is accurate and appropriate, and does not contain any confidential information about the school, its parents, pupils or staff.

- The school recognises the value of using social media for school purposes to enhance learning and ameliorate communication and engagement of parents. Staff must follow the guidelines of this document when using social media: recognisable images of children may only be used with the parents' permission; pupil surnames must not be published; when using social media in the classroom content must be checked carefully by staff before use.

- Staff should not communicate with parents or pupils using their personal mobile telephones. In the infrequent scenario where multiple school phones are needed by staff (Parent consultations evenings, etc.), staff may choose to use their personal mobile phones to communicate with parents if there is no extra charge. Staff must ensure that their number is hidden from the caller. This can be amended in your phone's settings by turning off 'Caller ID'. Always check by calling a trusted party before making a call to a parent /carer, to ensure that your number is hidden when calling.

- Staff should not request, or respond to, any personal information from a pupil other than that which might be appropriate as part of their professional role: communication outside of agreed protocols may lead to disciplinary and/or criminal investigations.

- Staff are able to access work email and the Internet at home using the school laptops and iPads but must ensure that they do not download software or programs from the Internet, or open emails that could contain viruses when at home.

- Cyberbullying (using technology to embarrass, humiliate, threaten or intimidate) is dealt with in the same way as bullying at Corsham Primary School – please see Corsham Primary's Anti-bullying policy: records should be kept, and teacher/line manager informed of the incidences so they can be recorded and dealt with appropriately. Corsham Primary School Behaviour Policy is also followed in any cases of misuse of social media by children where members of staff are misrepresented and police investigation will be considered. Pupils are taught about cyberbullying through PSHEE lessons.

Teaching and learning

- Internet access will be planned to enrich and extend learning activities - access levels will be reviewed to reflect curriculum requirements.

- Staff will select sites which will support learning outcomes planned for pupil's age and maturity. Children in Key Stage 2 will be required to use search engines to locate websites and information, but this will be carried out with adult supervision.

- Teachers are responsible for guiding pupils in their online activities, by providing clear objectives for Internet use - teaching staff will also ensure that pupils are aware of what is regarded as acceptable and responsible use of the Internet.

- Pupils (at an appropriate level) will be made fully aware of the risks to which they may be exposed while on the Internet - they will be shown how to recognise and avoid the negative aspects of the Internet such as pornography, violence, racism and exploitation of children, through PSHEE, e-Safety and Circle Time lessons.

- Specific e-safety lessons are taught at least once a year in every year group through Jigsaw, our PSHEE scheme of learning.

- Planned seating and computer monitor positions will allow teachers to observe, trace and monitor pupil access and usage of the Internet. Internet 'History' checks can be used to monitor Internet activity of pupils whilst using the Internet.

- All Internet access is filtered through a proxy server to screen out undesirable sites.

Tablets e.g. iPads

- iPads are available across the school – exactly the same 'acceptable use' rules apply to these devices.

- As it is easier to use these devices inappropriately without being detected, pupils are encouraged to be vigilant and responsible, and alert an adult immediately if any inappropriate use takes place.

- Pupils must ask permission before using their tablet e.g. iPad, or a digital camera, to photograph another pupil or staff member.

- Teaching staff will regularly discuss appropriate use with pupils and remind them of the sanctions that will result following inappropriate use: loss of Golden Time, followed by a reminder of the Acceptable Use Policy; repeated offences will result in the Internet being removed from an individual's iPad followed by a parental meeting.

Seesaw and Tapestry

- At Corsham Primary School we use software applications that allow pupils and teachers to publish learning online.

- Seesaw enables pupils to upload learning on school devices, allowing them to develop an online e-portfolio space, take part in discussions, contribute to collaborative wikis, communicate with peers and teachers online and engage in focussed learning tasks as the teacher is able to set learning for them to do.

- Content uploaded to Seesaw and Tapestry is monitored, checked and accepted by class teachers. Teachers can refuse to accept the uploading of work, pupil's comments and parent comments if it is not deemed appropriate.

- Letters are sent home to parents at the beginning of the year, outlining the purpose of Seesaw and Tapestry, how to connect to their child's portfolios and appropriate use.

- These letters also ask parents / carers for permission for their child to be included in group photos with other pupils.

School Website & TV Screens

- The copyright of all material on the school's web pages belongs to the school – permission to reproduce any material must be sought and obtained.

- Contact details for the school will include only the school's postal address, e-mail address and telephone number – no information about teachers', governors' or pupils' home addresses or the like will be published. Pupil surnames will not be published.

- The school will not publish any material produced by individual or groups of pupils to the website or TV screens without the agreed permission of their parents in line with the school's photographic permissions policy.

- Identifiable photographs of pupils whose parents have not provided written permission will not be published to the website – a pupil's full name will not be used in association with any photograph.

- Video footage of pupils published to the website or TV screens will not be published if parents' written permission has not been provided

Bringing Your Own Device (BYOD) to School

- Personal devices brought to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.

- School staff, authorised by the Head of School may search pupils or their possessions and confiscate any device they believe is being used in an inappropriate manner. If it is suspected that the device contains material related to a criminal offence the device will be handed over to the Police.

- Sending abusive or inappropriate messages or content is forbidden.

- BYOD devices are not permitted to be used in certain areas or situations, e.g. whilst changing is happening, in toilets, in situations of distress etc.

- BYOD will not be used for staff and pupils to contact each other.

- Access to the internet on BYOD devices will be through the schools wireless, filtered internet service – devices will use the 'SWGfL' and 'Soft Egg' proxy settings to ensure safe Internet access during school time.

- The school will monitor the use of the devices as it deems appropriate.

Zoom / Microsoft Teams / Other video calling services

- Video calling can be used to communicate effectively with other members of staff within the school or MAT. The main purpose of using video calling should be for: staff training, staff meetings, collaboration with other members of staff, planning and assessment.

- When on a video call, ensure that no other parties are present. If unknown parties are present and cannot be identified, simply end the call as soon as possible and report this to your Head of School.

- Zoom video calling can be used for parental consultations. In this scenario, all calls should be recorded for safeguarding purposes, with the video being stored on a local hard drive (the user's computer) for up to 1 calendar month.

- The parties involved within the call must be informed that the call is being recorded for the purpose of safeguarding.

- When calling parents / carers, staff must be visible and a professional background and environment should be presented.

- Staff must ensure that the recipient's video is on and that no other parties are present within the call that should not be present.

- Zoom / Teams can be used within school to communicate with pupils for School Council, Eco Council, ICT Incredibles, Sports Leaders, etc.

- Zoom / Teams should not be used to communicate with pupils outside of school.

Communicating the AUP

- ‘Rules for responsible Internet use’ posters will be displayed near all networked fixed position computer systems.

- E-Safety lessons will be provided yearly and will include references to Acceptable Use of the Internet.

- Pupils will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet.

- All staff will be provided with a copy of the School’s Acceptable Use & e-Safety Policy – teachers are aware that Internet traffic can be monitored and traced to an individual user.

- Staff will be consulted regularly about the developments of the school’s Acceptable Use Policy and given instructions on safe and responsible use of the Internet.

- To avoid misunderstandings teachers will contact the Lead Computing Engineers regarding any doubts that arise concerning the legitimacy of any given instance of Internet use.

- All parents / guardians will be provided with a copy of this policy, (within the Parent Pack), informing them how we use the Internet at Corsham Primary and how we share the responsibility - parents will be invited to write to the school if they have any opposition to their children being taught online with these measures in place (this acknowledges that parents / guardians accept some responsibility for the way in which their children use the Internet and that in spite of all reasonable precautions and supervision there remains a small risk of children viewing inappropriate material). All comments on and suggestions concerning this Acceptable Use & e-Safety Policy should be sent to the Lead Computing Engineers via the school office.

Equal Opportunities

When writing and reviewing this policy staff have completed an Equality and Diversity Impact Assessment in order to ensure it complies with equality obligations outlined in anti-discrimination legislation. We believe the policy positively reflects the aims and ambitions identified in Corsham Primary’s Single Equality Scheme.

UNICEF

CPS is a UNICEF *Rights Respecting School* which promotes the Convention of the Rights of the Child. This policy underpins Article 29 of the convention:

Aims of Education: Education shall aim at developing the child's personality, talents and mental and physical abilities to the fullest extent. Education shall prepare the child for an active adult life in a free society and shall foster in the child respect for his or her parents, for his or hers cultural identity, language and values and for the cultural background and values of others.

Success Criteria

- The Lead Computing Engineers and Heads of School have ensured that a copy of this policy with a covering letter is given out to parents as part of their introduction pack.

- Teachers and Teaching Assistants are informed in INSET about this policy (inset timetables).

- Children have been supervised while using the Internet in class lessons (timetables and planning folders).

Policy Review

This policy will be reviewed annually.
This policy may be reviewed earlier at the discretion of the Governors or in the event of changes in policy or legislation at either governmental or LA level.