EVERSFIELD PREP SCHOOL

e-Safety Policy

November 2023

CONTENTS

Contents 2
Mission 3
Aims 3
INTRODUCTION 3
INTERNET ACCESS IN SCHOOL 3
WHY INTERNET USE IS IMPORTANT 4
HOW THE INTERNET BENEFITS EDUCATION 4
USING THE INTERNET TO ENHANCE LEARNING 4
HOW PUPILS WILL LEARN TO EVALUATE INTERNET CONTENT 5
MANAGING EMAIL 6
MANAGING WEBSITE CONTENT 6
PUBLISHING PUPILS' IMAGES AND WORK 7
MANAGING SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING 7
MANAGING EMERGING TECHNOLOGIES 7
PUPILS USE OF PERSONAL DEVICES 7
SCHOOL STAFF 8
HOW PERSONAL DATA SHOULD BE PROTECTED 8
HOW INTERNET ACCESS WILL BE AUTHORISED 9
HOW RISKS WILL BE ASSESSED 9
MANAGING FILTERING 9
HOW ICT SYSTEM SECURITY WILL BE MAINTAINED 9
HOW THE SCHOOL WILL RESPOND TO ANY INCIDENTS OF CONCERN 9
HOW E-SAFETY COMPLAINTS WILL BE HANDLED 10
CYBERBULLYING 10
HOW INTERNET IS USED ACROSS THE COMMUNITY 10
INTERNET USE AT HOME 11
INTRODUCING THE POLICY TO PUPILS 11
DISCUSSING THE POLICY WITH STAFF 11
ENLISTING PARENT/CARERS SUPPORT 11
Equal Opportunities 11
MONITORING AND REVIEW 12
APPENDIX A – USEFUL RESOURCES FOR TEACHERS AND PARENTS 13
    USEFUL RESOURCES FOR TEACHERS 13
    USEFUL RESOURCES FOR PARENTS 13
APPENDIX B – ESAFETY/ACCEPTABLE USE OF INTERNET RULES FOR STAFF AND PUPILS 14
APPENDIX C – ESAFETY/ACCEPTABLE USE OF INTERNET RULES FOR PUPILS 15
APPENDIX D – STAFF INFORMATION SYSTEMS CODE OF CONDUCT / ACCEPTABLE USE POLICY 16

MISSION

Eversfield offers an outstanding, broad education within a safe, caring, happy, family atmosphere where the talents of every child are valued and nurtured. We achieve excellent results in a school where the Christian principles of mutual care, respect and encouragement underpin everything that we do.

AIMS

- To promote high moral standards through clear and relevant Christian teaching.
- To provide a wide breadth of experiences and opportunities for all our pupils to discover and develop their individual talents.
- To support our pupils in becoming valued members of society so that they may develop self-confidence, ask questions, seek new experiences, not be afraid to make mistakes, express themselves confidently and modestly and develop team and leadership skills.
- To provide a safe, supportive, healthy educational environment, with buildings, facilities and staff that enable our pupils to learn and develop.
- To ensure that our pupils receive excellent pastoral care.

INTRODUCTION

This policy has been written by the Subject Leader of Computing/IT Network Manager and has been approved by the Headmaster. It outlines our purpose in providing electronic communications facilities at the school in the form of electronic mail and access to the Internet. It explains how the school has put in place safeguards to avoid the potential problems that unrestricted Internet access can give rise to.

This policy has been written with reference to:

- Child Protection and Safeguarding policies 2023
- Keeping Children Safe in Education (KCSIE) 2023
- Social Media policy
- UKCCIS Education for a connected world framework
- UK Safer Internet Centre
- CEOPS

INTERNET ACCESS IN SCHOOL

Providing access to the Internet in school will raise educational standards and support the professional work of staff. Staff and pupils will have access to websites world-wide offering educational resources, news and current events. There will be opportunities to communicate with and exchange information with pupils and others worldwide.

In addition, staff will have the opportunity to access educational materials and advisory and support services, communicate with professional associations and colleagues; exchange curriculum and administrative information and participate in government initiatives.

Staff will not be expected to take charge of an Internet activity without appropriate initial training. All staff have access to this e-Safety policy and will be reminded of the e-Safety Rules, which are visible in any room of the school where there is a computer.

Parents' attention will be drawn to the existence of the e-Safety policy and rules in the Parent Handbook; these will also be published on the school website. All children from Forms 1 to 6 are required to sign the school's e-Safety policy.

WHY INTERNET USE IS IMPORTANT

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is statutory curriculum and is a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn the knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

HOW THE INTERNET BENEFITS EDUCATION

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between students world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Access to learning wherever and whenever convenient.

USING THE INTERNET TO ENHANCE LEARNING

- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils and the curriculum requirements.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives of Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

ONLINE SAFETY

Eversfield identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content

being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct
personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

Commerce
risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The DSL has overall responsibility for online safety within the school/college but will liaise with other members of staff, for example IT staff, curriculum leads etc. as necessary. The DSL will respond to online safety concerns reported in line with our child protection and other associated policies, including our anti-bullying, social media and behaviour policies.

- Internal sanctions and/or support will be implemented as appropriate.

- Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

HOW PUPILS WILL LEARN TO EVALUATE INTERNET CONTENT

- If staff or pupils discover (view) unsuitable sites, the URL (address) and content must be reported to the IT Network Manager immediately. The website in question will be added to Eversfield's URL Filtering System.
- The school should ensure that the use of Internet derived materials by staff and by pupils complies with the copyright law.
- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television.
- Pupils in Forms 1-6 will be reminded of the school's e-Safety policy at the start of each academic year.
- The new curriculum takes a drip feed approach to teaching e-safety, with the children being reminded of the e-safety rules and looking at how to stay safe when using technology at varying times throughout the year. The table below highlights the occasions when this should be done within the curriculum:

Year	**Michaelmas**	**Lent**	**Summer**
Nursery		Unit N4 – Stranger Danger	
Reception	Unit R2 – Posting images on line	Unit R4 – Stranger Danger	
Year 1		Unit 1.3 – Giving out personal information	Unit 1.5 – Posting images on line
Year 2	Unit 2.1 – On line foot print	Unit 2.3 – Your virtual self	
Year 3		Unit 3.3 – Posting images on line	Unit 3.5 – Searching on line
Year 4	Unit 4.1 – Social Media		Unit 4.6 – Your virtual self
Year 5	Unit 5.1 – Posting images on line	Unit 5.5 – Social media and blogging	
Year 6	Unit 6.2 – Apps (permissions, ratings, age, settings, purchases)		

These areas should not be seen as the only opportunities that e-safety can be taught to the children, but offer the minimum expectation within the curriculum.

- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium).
- Pupils will be made aware that the writer of an email or the author of a web page may not be the person claimed.

MANAGING EMAIL

- Pupils will only be allowed to use email once they have been taught the *Rules of Responsible Internet Use* and the reasons for these rules.
- Teachers will endeavour to ensure that these rules remain uppermost in the pupils' minds as they monitor them using email.
- Pupils may send email as part of planned lessons and will be given an individual email address.
- Pupils may only use approved email accounts on the school system.
- Where known, access in school to external email accounts is blocked. As further email accounts are made known, these will also be blocked by the IT Network Manager.
- Staff will only use official school provided email accounts to communicate with pupils and parent/carers, as approved by the Leadership Team.
- Both incoming and outgoing email to pupils may be read by teachers and the IT Network Manager.
- Regular checks on incoming and outgoing emails will be taken by the IT Network Manager and Subject Leader of Computing.
- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number or arrange to meet anyone.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Emails sent to an external organisation must be authorised by a teacher before sending.
- Children will only use their school email on the school premises. This email is not to be used for organising social activities outside of school.
- The forwarding of chain messages will not be permitted.

MANAGING WEBSITE CONTENT

- The point of contact on the website should be the school address, school e-mail and school telephone number. Staff or pupil's home information will not be published.
- Website photographs that include pupils will be selected carefully to ensure permission has been given by parents.
- The Marketing Manager, working with the Headmaster will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Class teachers will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained.
- All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- The Marketing Manager is responsible for uploading pages to the school website, ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

- Parents are able to access information specifically for current parents via a password protected page. The password is changed annually.

PUBLISHING PUPILS' IMAGES AND WORK

- Images or videos that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website in association with photographs.
- When a pupil joins the School, parental consent is requested regarding the use of pupil photographs/videos to be used on the school website/Twitter, in school publications and for marketing purposes.
- Written consent will be kept by the school where pupil images/videos are used for publicity purposes.
- Parents are not informed individually before publishing photographs/videos and/or samples of children's work on the school website.

MANAGING SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

- As part of the Computing curriculum, children will be taught how to use some types of social media, such as a Wiki. When working on these topics in school, every effort has been taken to ensure the safety of the children and as such the sites used are of a 'walled garden' in nature. Other social media and social networking sites, such as Facebook, will be blocked by the IT Network Manager. Any sites which have not been blocked must be reported to the IT Network Manager immediately.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of family/friends, specific interests and clubs etc.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the site terms and conditions to ensure the site is age appropriate.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parent/carers, particularly when concerning pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing will be subject to the school's Social Media Policy.

MANAGING EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not permitted to have mobile phones, tablet devices, smart watches or location trackers (such as Apple AirTags) within school.
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. These should not be used within school.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

PUPILS USE OF PERSONAL DEVICES

- If the pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parent/carers in accordance with the school policy.
- If a pupil needs to contact his/her parent/carers they will be allowed to use the school phone.

STAFF USE OF PERSONAL DEVICES

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting of a professional capacity. Staff are now encouraged to have their own phones during activities in case of emergencies.
- Mobile phones and devices will be switched off or switched on 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place if approved by the Leadership Team.
- Staff are encouraged to use school provided equipment to take photos or videos of pupils, but may use personal devices such as mobile phones or cameras provided that images are transferred onto the school network as soon as conveniently possible and deleted from the personal device once transferred.
- If a member of staff breaches the school policy then it will be viewed as a disciplinary issue.

SCHOOL STAFF

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff taken from the Department of Education document, 'Cyberbullying: Advice for Teachers and School Staff' (November 2014) which may help protect your online reputation:

- Ensure you understand your school's policies on the use of social media, Childnet's 'Using Technology' guide has more information on what to be aware of.
- Do not leave a computer or any other device logged in when you are away from your desk. Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils. All school computers should be locked when not in use.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer internet advice and resources for parents and carers.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation minisite has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from pupils past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school's contact details.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

HOW PERSONAL DATA SHOULD BE PROTECTED

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

HOW INTERNET ACCESS WILL BE AUTHORISED

- The school will maintain a record of any pupils whose parent/carers have specifically denied internet or e-mail use.
- By using the Internet, staff and pupils are agreeing to abide by the e-Safety Policy.
- All staff will read and sign the Staff Information Systems Code of Conduct before using any school IT resources.
- Parent/carers will be asked to sign and return e-Safety Rules form stating that they have read and understood the e-Safety Policy and Rules. A sample is contained in Appendix A of this document.
- All visitors to the school site who require access to the school network or internet access will be asked to read and sign the Staff Information Systems Code of Conduct. The form is available from the IT Network Manager.

HOW RISKS WILL BE ASSESSED

- In common with other media such as magazines, books and videos, some material available on the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users only access appropriate material. However due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The IT Network Manager/Subject Leader of Computing will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

MANAGING FILTERING

- The school's internet access will include filtering appropriate to the age and maturity of pupils.
- The filtering system contains blocking strategies which prevent access to unsuitable sites. This is maintained by the IT Network Manager.
- The IT Network Manager/Subject Leader of Computing will ensure unsuitable sites have been blocked.
- If staff or pupils discover (view) unsuitable sites, the URL (address) and content must be reported to the ICT Network Manager immediately. The website in question will be added to Eversfield's URL Filtering System.
- Any material thought to be illegal will be referred to the Internet Watch Foundation and the Police.

HOW ICT SYSTEM SECURITY WILL BE MAINTAINED

- The school ICT systems will be reviewed regularly in regard to security.
- Virus protection will be installed and updated regularly on all computer systems
- Pupils are not permitted to bring in any form of external storage devices such as USB, hard-drives.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school network will be regularly checked.
- The IT Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

HOW THE SCHOOL WILL RESPOND TO ANY INCIDENTS OF CONCERN

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc).

- The DSL will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parent/carers of any incidents of concerns as and when required.
- After investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

HOW E-SAFETY COMPLAINTS WILL BE HANDLED

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any compliant about staff misuse must be referred to the Headmaster.
- Pupils and parent/carers will be informed of the complaints procedure.
- Parent/carers and pupils will need to work in partnership with the staff to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which could cause harm, distress or offence to any other members of the school community.

CYBERBULLYING

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse disciplinary or criminal procedures may apply.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.

Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the Senior Leadership Team, and their union representative if they are a member. The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

HOW INTERNET IS USED ACROSS THE COMMUNITY

- Any member of staff using the school computer system will need to sign the acceptable use policy.
- Parent/carers of children will be required to sign an acceptable use policy on behalf of the child. Please see the sample form later in this document.

- The school will provide an Acceptable Use Policy for any visitor who needs to access the computer system or internet on site.

INTERNET USE AT HOME

- Parent/carers are responsible for e-Safety outside school and should be aware of what is being accessed by their children.
- Parent/carers who are concerned with internet security and other e-safety issues can email school on esafety@eversfield.co.uk or contact the Headmaster.

INTRODUCING THE POLICY TO PUPILS

- The Rules for Internet access will be posted in all rooms where computers are used and discussed with pupils regularly.
- In Forms 1 to 6 the children will be reminded of the Acceptable Use of Internet rules at the start of each academic year.
- All pupils will be informed that network and Internet use will be monitored.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- E-Safety training is embedded within the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum.

DISCUSSING THE POLICY WITH STAFF

- All staff will be provided with the school e-Safety policy, and its importance explained.
- To protect staff and pupils, the school will implement Acceptable Use Policies.
- All staff are governed by the terms of the Staff Information Systems Code of Conduct Form that must be signed.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

ENLISTING PARENT/CARERS SUPPORT

- Parent/carers' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively to inform parent/carers without undue alarm.
- A partnership approach with parent/carers will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Parent/carers will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Interested parent/carers will be referred to organisations listed at the end of this document.

EQUAL OPPORTUNITIES

We are committed to the principle of equal opportunity for all pupils irrespective of race, religion, gender, language, disability or family background, and to the active support of initiatives designed to further this principle.

We believe that equal opportunity is at the heart of good educational practice. All pupils are of equal value and deserve equal access to every aspect of school life. They have an equal opportunity to learn and work towards their highest possible levels of achievement. The 'Vision and Values' which we uphold as a school help to emphasize equal opportunities for all staff and pupils at all times. All personnel are responsible for ensuring that we implement this policy.

MONITORING AND REVIEW

This Policy is monitored by the Governing Body and will be reviewed every three years or earlier, if deemed appropriate.

MN, SL Computing & IT Network Manager, revised November 2023

APPENDIX A – USEFUL RESOURCES FOR TEACHERS AND PARENTS

USEFUL RESOURCES FOR TEACHERS

- BBC Own IT https://www.bbc.com/ownit
- Child Exploitation and Online Protection Centre www.ceop.police.uk/
- Childnet www.childnet-int.org/
- Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
- Education for a Connected World https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF
- SWGfL https://swgfl.org.uk/resources/
- Think U Know www.thinkuknow.co.uk/
- UK Safer Internet Centre https://www.saferinternet.org.uk/

USEFUL RESOURCES FOR PARENTS

- BBC Own IT https://www.bbc.com/ownit
- Family Online Safe Institute www.fosi.org
- Internet Matters https://www.internetmatters.org/
- Internet Watch Foundation www.iwf.org.uk
- Parent Info https://parentinfo.org/
- Parent Zone https://parentzone.org.uk
- Think U Know www.thinkuknow.co.uk/
- UK Safer Internet Centre https://www.saferinternet.org.uk/

APPENDIX B – ESAFETY/ACCEPTABLE USE OF INTERNET RULES FOR STAFF AND PUPILS

Eversfield Preparatory School

e-Safety/Acceptable use of internet rules for Staff and Pupils

The school has a mixture of computers and iPads with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the Computers:

- The school IT systems may not be used for private purposes, unless the Headmaster has given specific permission.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Accessing other people's files is not permitted.
- Pupils are not permitted to use external sources such as memory sticks, on the school network without permission of the IT Manager.
- Use of financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Using the Internet to browse Web pages:

- I will ask permission from a teacher before using the Internet to browse Web pages.
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself
- I understand that the school checks my computer files and will monitor the Internet sites I visit.
- I will not complete and send web based forms which request personal information.

Using Email:

- I will ask permission from a teacher before checking my Email account.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.
- I understand that Email messages I receive or send may be read by the IT Network Manager/Subject Leader of Computing.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- I will only send Email messages to people that my teacher has approved.
- I will not give my home address or telephone number on an Email message.
- I will not use Email to arrange to meet someone outside school hours.

APPENDIX C – ESAFETY/ACCEPTABLE USE OF INTERNET RULES FOR PUPILS

Eversfield Preparatory School

e-Safety/Acceptable use of internet rules for Pupils

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parent/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

PUPIL NAME		**FORM**	

Pupil's Agreement

I have read and understand the school e-Safety Rules.

I will use the computer, network, Internet access and other new technologies in a responsible way at all times.

I know that network and Internet access can be monitored.

SIGNED		**DATE**	

Parent/Carer's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and videos that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupils full names.

Parent/Carer's Consent for Internet Access

I have read and understood the school e-safety rules and given permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of Internet facilities.

SIGNED		**DATE**	

Please print name :

Please complete, sign and return to the school

APPENDIX D – STAFF INFORMATION SYSTEMS CODE OF CONDUCT / ACCEPTABLE USE POLICY

Eversfield Preparatory School

STAFF INFORMATION SYSTEMS
CODE OF CONDUCT / ACCEPTABLE USE POLICY

To ensure that staff are fully aware of their professional responsibilities when using the IT systems, they are asked to sign the code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

STAFF NAME	

- Any computer/device that I have been given and the IT systems that I use belong to the school and I understand that it a criminal offence to use a computer for a purpose not permitted by its owner (Eversfield Preparatory School).
- I will ensure that my use of the school's IT systems, including all devices, will always be compatible with my professional role.
- I understand that the school's IT systems may not be used for private purposes, without specific permission from the Headmaster.
- I understand that the school may monitor my school computer and Internet usage to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than the IT Network Manager if required.
- I will not install software without permission of the IT Network Manager.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Co-ordinator or the DSL.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them develop a responsible attitude to system use and to the content they access or create.

The school may exercise its rights to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's IT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I confirm that I have read, understood and agree with the e-Safety Policy including the e-Safety rules and Information Systems Code of Conduct.

SIGNED		**DATE**	

When submitted electronically and without personal signature, electronic receipt of this form by the School will be deemed equivalent to the submission of a signed version and will constitute confirmation of the declaration above.

Please complete, sign and return to the School Office ASAP