Online Safety Policy

Title:	Online Safety Policy
Document Reference:	**S-15**
Issue Date:	June 2026
Next Review Date:	June 2027
Issue:	03

DOCUMENT AUTHORITY		
Prepared by:	Alex Pickerden / Laura Howard	DSL / Online Safety Lead Teacher
Approved by:		

DOCUMENT HISTORY			
Issue No	**Reason for Change**	**Page(s) affected**	**Date**
3	Updates to statutory guidance and legislation	3	June 2026
3	Updates to school staff and responsibilities	3, 6	June 2026
3	Changes to curriculum offer (PSHE / Pol-Ed / Project Evolve)	5	June 2026
3	Storage updated to include Seesaw	8	June 2026
3	Changes to guidance around definitions and terminology	8	June 2026
3	Updated User Agreements (Staff and Pupils)	Appendices	June 2026

Contents

1. **Aims**
2. **Legislation and Guidance**
3. **Teaching and Learning**
4. **Curriculum Objectives**
5. **Relationships, Sex and Health Education (RSHE)**
6. **GDPR, Data Protection, Security and Safeguarding**
7. **Roles and Responsibilities**
   - **7.1 DSL/DDSL**
   - **7.2 All Staff and Volunteers**
   - **7.3 Parents / Carers**
8. **Implementation: Practicalities, Decisions and Logistics**
   - **8.1 Electronic Communication**
   - **8.2 Social Networking and Publishing**
   - **8.3 Children's Use of the Internet**
   - **8.4 Mobile Technology Management**
   - **8.5 Online Communication and Safer Use of Technology**
   - **8.6 Cyberbullying**
   - **8.7 Artificial Intelligence**

8.8 Storage

9. Acceptable Use of Internet, Technology and Devices

9.1 Acceptable Use of the Internet in School

9.2 Responding to Online Incidents and Safeguarding Concerns

9.3 Staff Personal Use of social media

9.4 Pupil Use of social media

9.5 Staff Use of Personal Devices and Mobile Phones

9.6 Pupil Use of Personal Devices and Mobile Phones

9.7 Visitors use of personal devices and mobile phones

10. Related Policies

Appendices

Be Smart Online

Acceptable User agreement for EYFS + KS1

Acceptable User agreement for KS2

Acceptable User agreement for staff

1. Aims

At Yarborough Academy we believe that technology and computing is at the heart of the curriculum. We want to equip our children to participate in a rapidly changing technical world where work and leisure activities are increasingly transformed by technology. We recognise the Online Safety issues, especially those linked to developing and emerging technologies such as Artificial Intelligence (AI) and plan accordingly to ensure appropriate, effective and safe use of electronic communications and resources.

The school aims to provide the right balance between controlling access to the Internet and technology, setting rules and boundaries and educating students and staff about responsible use. The school understands that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children are empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff are aware of the importance of good Online Safety practice in the classroom in order to educate and protect the children in their care. Members of staff are expected to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. It is crucial that all staff are aware of the offline consequences that online actions can have.

The breadth of issues related to online safety are ever evolving but as outlined in the statutory guidance KCSIE 2025 can be categorised into four areas of risk- content, contact, conduct and commerce. These four categories will form the basis of this policy:

*__Content__ – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

*__Contact__ – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes

*__Conduct__ – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

*__Commerce__ – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

- The school has appointed an Online Safety Lead / Deputy Safeguarding Lead (Miss L. Howard) who liaises closely with the Designated Safeguarding Lead (Mr A. Pickerden) and other Deputy Safeguarding Leads (Mrs L. Walton and Mrs. S Kiss)
- The Online Safety Policy and its implementation will be reviewed annually.
- Our Online Safety Policy has been written by the school, building on government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by the board of Trustees.
- The Board of Trustees will discuss Online Safety issues as part of the Safeguarding Agenda items.
- Online Safety is also discussed weekly in the SWAT meetings held by the safeguarding team in school.

2. Legislation and guidance

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

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

3. Teaching and Learning

- Internet use is part of the statutory National Curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school so we teach them how to evaluate what they see online, how to recognise techniques used for persuasion, understand what acceptable and unacceptable online behaviour looks like, identify online risks, to take care of their own safety and security and how to seek support and when to seek support.
- 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.
- The school's Internet access will be designed to enhance, extend and provide educational opportunities.
- Teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.
- Pupils will be given clear objectives for keeping themselves safe online including cybercrime. Due regard will be given to children with Special Education Needs.
- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, how to locate, retrieve and evaluate knowledge safely.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

4. Curriculum Objectives

- The curriculum includes clear learning objectives that are taught and assessed in order to give children the ability to connect with others safely and respectfully, understanding the need to act within the law and with moral and ethical integrity.
- Key Stage One breadth of study: Communicate safely and respectfully online, keeping personal information private and recognise common uses of information technology beyond school.
- Key Stage Two breadth of study: Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Milestone One (Year 1 and 2) – To connect: Participate in class social media accounts; Understand online risks and the age rules for sites.
- Milestone Two (Year 3 and 4) – To connect: Contribute to blogs that are moderated by teachers; Give examples of the risks posed by online communications; Understand the term 'copyright'; Understand that comments made online that are hurtful or offensive are the same as bullying; Understand how online services work.
- Milestone Three (Year 5 and 6) – To connect: Collaborate with others online on sites approved and moderated by teachers; Give examples of the risks of online communities and demonstrate knowledge of how to minimise risk and report problems; Understand and demonstrate knowledge that it is illegal to download copyrighted material, including music or games, without express written permission, from the copyright holder; Understand the effect of online comments and show responsibility and sensitivity when online; Understand how simple networks are set up and used.
- PSHE topics are taught through Pol-Ed across the school and PSHE association – Year 1: Keeping safe; What is private information; How can I be responsible with AI. Year 2: What are the risks of video gaming; How can I be safe Online; Screen Free Time. Year 3: What are the risks of online challenges; Creating and managing passwords with different devices; Digital deception and deepfakes. Year 4: Internet safety: Age restrictions; Keeping safe online.

Year 5: What can and can't I do on the internet; Media influence; Deepfakes; Online image; How might being online impact how I feel. Year 6: Critical digital consumers; Social media; Online reputation; Pressure and technology.

- Additional Online Safety topics are taught in every year group from Year 1-6: This is completed through the Project Evolve Programme. These topics include: Self-image and identity, Online Relationships, Online Bullying, Heath Wellbeing & Lifestyle, Privacy & Security, Copyright and Ownership, Managing Online Information.

5. Relationships, Sex and Health Education (RSHE)

As outlined within the 'Keeping Children Safe in Education' statutory guidance, children will also be taught about Online Safety through RSHE sessions.

RSHE guidance sets out clear online safety expectations. At Yarborough Academy the online safety content that will be taught through RSHE sessions will include the following aspects. This is not an extensive list and more of the RSHE curriculum will link closely to Online Safety.

Respectful Relationships

- About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help.

Online Relationships

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.

Being Safe

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Mental Wellbeing

- That bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing.
- Where and how to seek support (including recognising the triggers for seeking support), including whom in school they should speak to if they are worried about their own or someone else's mental wellbeing or ability to control their emotions (including issues arising online).

Internet Safety and Harms

- Understanding that for most people the internet is an integral part of life and has many benefits.
- About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Why social media, some computer games and online gaming, for example, are age restricted.
- That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- Where and how to report concerns and get support with issues online.

6. GDPR, Data Protection, Security and Safeguarding

The Schools broadband is protected by a firewall and filtering via TSS (Technology Support Solutions Ltd.)

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Confidential information / personal data sent over the Internet or accessed off site will be password protected (through Google email accounts and Google Drive) or via MOVE IT if necessary.
- Remote access to the school server will be via a safe system (VPN).

- The use of user logins and passwords to access the school network will be enforced.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Data is protected with secure username and password.
- Websites are strategically allowed or blocked using Smoothwall.
- If staff or pupils discover unsuitable sites, the URL will be blocked by TSS Services.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list via Smoothwall.
- Any Online Safety issues are reported directly to the Online Safety Lead and Safeguarding Lead as per the CP/Safeguarding Policy.
- Teachers work closely with the designated Online Safety and Safeguarding lead to ensure all safeguarding incidents online are dealt with following the schools safeguarding procedures.
- Images and names of staff will appear on the school website. Staff have the right to have any image or their name removed from the school website. Personal information regarding staff members will not be shared.
- Images of staff will be removed from the school website once the member of staff has left the school. Any digital media of the member of staff will also be removed from the website cache.
- Parents have the right to request the removal of images of their child from the school website and ask where images of their child, for the purpose of the website, is held.

7. Roles and Responsibilities

7.1 Designated Safeguarding Lead and Deputies (DSL/DDSL)

- To lead on the filtering and monitoring system with the use of IT with the close support of the online safety lead and ICT manager (TSS).
- Keep up-to-date with current research, legislation and trends regarding online safety.
- Work alongside the wider safeguarding team (SWAT) to ensure any online safeguarding incidents are investigated following the schools safeguarding procedures.
- To provide resources for regular (at least annual) training and updates to all staff on Online Safety.
- To ensure new staff have access to online safety training during induction.
- To ensure Trustees receive Online Safety training.
- Work closely with the Designated Data Protection Officer to ensure all online apps/services are GDPR compliant.
- Act as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety.
- Coordinate participation in local and national events to promote positive online behaviour.
- Ensure that online safety is promoted to parents and carers and the wider community.
- Work with stakeholders to ensure that data protection and security meets current legislation.
- Monitor the school online safety incidents to identify gaps and use the education response to reflect need.
- To report to the School Leadership Team and Trustees any concerns about online safety.

7.2 All Staff and Volunteers

- Contribute to the development of online safety policies.
- Implementing this policy consistently and with understanding.
- Take responsibility for the security of school systems and data.
- Have an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Model good practice when using new and emerging technologies
- Embed online safety in curriculum delivery wherever possible.
- Identify individuals of concern and take appropriate action by following school safeguarding policies and procedures.
- Know when and how to escalate online safety issues. Including knowledge of who the DSL/ DDSLs at the academy are.
- Be able to signpost to appropriate available support.
- Maintain a professional level of conduct in their personal use of technology both on and off school site.
- Read and accept the Acceptable User Policies (AUPs) (See Appendices)
- Undertake regular (at least annual) training/ updates on Online Safety.

7.3 Parents/Carers

- Notify the headteacher of any concerns or queries regarding this policy.
- Ensure their child had read, understood and agreed to the terms on acceptable use of the schools ICT systems and internet (See Appendices)
- Work in partnership with the academy to ensure children are using the internet and online devices safely and responsibly.

8. Implementation: Practicalities, Decisions and Logistics

8.1 Electronic Communication

- Pupils have monitored access to approved communication systems, which are rigorously monitored and used, only for school purposes.
- Pupils must immediately tell their teacher if they receive offensive messages.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use ParentMail, Tapestry and school accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Text messages and emails will be sent using the appropriate system (ParentMail) and always in a professional context.

8.2 Social Networking and Publishing

- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Images will only be published where parental consent has been given.
- Pupils' full names will not be used when publishing unless explicit permission from parents has been granted, particularly in association with photographs.
- Images or videos that include pupils will be selected carefully. For example, only images of pupils in suitable dress will be used in order to reduce the risk of inappropriate use.
- Images of learning are shared via the school website.

8.3 Children's Use of the Internet and Technology

- The school will control access to social media and social networking sites operating in full accordance with any Social Media restrictions for pupils introduced by the UK Government.
- Pupils will be advised never to give out personal details of any kind, which may identify them and/or their location.
- Any videoconferencing will always be prearranged with the organisation involved and always supervised by a teacher.

8.4 Mobile Technology Management

- Mobile devices will be used for educational benefit.
- Guided access (locking children into an app) will be used on iPads when appropriate.
- The Computing Lead / and ICT manager (TSS) have full control of downloading apps through secure passwords to stop children accessing inappropriate apps.
- All iPads are enrolled into lightspeed (mdm) and can be monitored at any time.
- Teachers will monitor the content of children's iPads to ensure appropriate educational use at all times.
- Weekly reports from TSS will be reviewed and monitored by the DSL and DDSL/Online Safety Lead to pick up on any inappropriate internet searches/ usage from both staff and pupils.

8.5 Online Communication and Safer Use of Technology

- The school will ensure that information posted on the school website meets the requirements identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published and ensure that the information is accurate and appropriate.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

- The school will post information about safeguarding, including online safety, on the school website.
- The school will ensure that all images and videos shared on the school website meets the school image use policy and permission from parents/carers is obtained.

8.6 Cyberbullying

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

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- To help prevent cyberbullying, we will ensure pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so.
- Pupils are taught to report anything that makes them feel uncomfortable in any way. Teaching staff are also encouraged to use all aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education and other subjects such as RSHE, Computing and Technology.
- All staff are trained on cyberbullying, its impacts and ways to support pupils, as part of regular safeguarding training and updates.
- In relation to a specific incident of cyberbullying, the school will follow the behaviour and relationships policy as appropriate. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.7 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Yarborough Academy recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Yarborough Academy will treat any use of AI to bully pupils very seriously, in line with our Behaviour and Relationships policy

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the academy and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

8.8 Storage

- Images of children that are to be stored will be done so on the academy secure server.
- Some children's work will be stored on Google Drive which is password protected, encrypted and can be accessed by pupils and staff only.
- Seesaw will also be used to store pupils' work and this platform is also protected through passwords which can be managed by staff only.
- The use of USB sticks to transfer sensitive or personal information with regards to children is forbidden.
- Any external storage devices used in school must have been purchased by the school and encrypted.

9. Acceptable Use of Internet, Technology and Devices

9.1 Acceptable Use of the Internet in School

- All staff will read and sign the School Acceptable Use Policy before using any school ICT / Computing resources.
- Staff will promote the Online Safety rules for pupils.
- Parents will be asked to read the Online Safety rules for pupil access and discuss it with their child, where appropriate.

- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Staff personal use of social networking, social media and personal publishing sites is discussed and safe and professional behaviour will be outlined in the Staff Code of Conduct.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Everyone in school is regularly made aware of Online Safety issues.
- Emerging technologies will be examined for educational benefit and the Online Safety Lead will ensure that appropriate risk assessments are carried out before use in the school.
- The school will audit any technology used to establish if the Online Safety Policy is adequate and the implementation of the policy is appropriate.

9.2 Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.
- If there is a possibility that an offence has occurred then any equipment used should be isolated and left unused to preserve any evidence on the device.
- Complaints about Internet / device misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher and dealt with in accordance with the Staff Code of Conduct and staff disciplinary procedures .
- Any allegations against a member of staff's online conduct will also be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- 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.
- 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 cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school Behaviour and Relationships policy where appropriate.
- The school will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken or is taking place, then the school will contact Humberside Police.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Humberside Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

9.3 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal sites is discussed with all members of staff as part of their induction and regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of the school community in the school Acceptable Use Policy and Staff Code of Conduct.
- Staff are advised not to communicate with or add to their network, any past or current pupils and family members via any social media channel. Any pre-existing relationships or exceptions may compromise this and should be discussed with the Headteacher.
- Any communication from a parent, pupil or pupils' family member must be reported to the Safeguarding Team (SWAT).
- The DDSL/Online Safety Lead will assess any communication from a parent, pupil or pupils family member and escalate if required to the Headteacher.
- All members of staff are strongly advised to safeguard themselves on all social media sites by making their accounts private. This also includes being aware of location sharing services, privacy levels, opting out of public listings and keeping personal information private.
- Members of staff are not encouraged to identify themselves as employees of Yarborough Academy through social media.

9.4 Pupil Use of Social Media

- Safe and responsible use of social media will be outlined for children and parents as part of the Acceptable Use Policy. The policy will also adopt any amendments linked to the UK Government's Social Media restrictions for pupils.
- All social media sites are blocked by default and will only be available to children after a thorough risk assessment carried out by class teachers. The Online Safety Leader will assess the educational benefits and monitoring facilities before opening any social media website/app up.
- Personal publishing on social media will be taught to pupils as part of a progressive education approach via age appropriate sites, which have been risk assessed and approved for education purposes.
- Pupils will be advised not to meet any online friends without a parent/carer.
- Pupils will be advised on appropriate security on social media sites.
- Pupils will be advised to consider the risks of talking to unknown people.
- Pupils will be advised to speak to their class teacher if they feel unsafe online.
- Parents are regularly updated with the latest news on social media sites.
- Any concerns regarding pupils' use of social networking at home will be dealt with in accordance with existing school policies including Behaviour and Relationships and CP/Safeguarding.

9.5 Staff Use of Personal Devices and Mobile Phones

- Members of staff are not to use personal laptops or PCs in school.
- The school employs a firewall and levels of access so that should personal devices be brought into school, they are unable to access school data.
- Any electronic devices of all kinds that are brought in on site are the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.
- Mobile phones should be switched off or on silent and out of sight during lesson times except under exceptional circumstances, which have been discussed with the Senior Leadership Team.
- Staff must ensure they use their mobile phone in a way that does not bring the school or profession into disrepute.
- Bluetooth or other forms of communication should be hidden or switched off.
- The sending of abusive or inappropriate messages or content via mobile phones is forbidden by any member of the community and any breaches will be dealt with through the Staff Code of Conduct and Staff Disciplinary policy.
- Members of staff will be issued with a work email address and encouraged to use the school telephone to make calls. If personal phones are used, the number must be withheld.
- Staff should only take photographs of children on personal devices where access to wireless networks is unavailable and photographs are to be used for school purposes. Permission for this must be sought beforehand from the Headteacher. Once used, these photographs must be removed from personal devices immediately.
- Staff using personal devices to access school email should implement 2-step verification by downloading and using the Gmail app.
- Staff should not use school Apple IDs and icloud facilities on their mobile devices to avoid photo-sharing capabilities.

- Guest Wi-Fi logins will be provided to staff who require Internet access on their personal devices. This is for emergency communication purposes. Codes will be given that expire after a set amount of time. If a member of staff leaves the academy, the ICT manager (TSS) can remove personal devices from the Wi-Fi.

9.6 Pupils Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices.
- We ask that pupils do not bring their own devices or mobile phones into school. The only exception being, if older children walk to school by themselves and have a phone for safety reasons.
- Any personal device brought into school should be switched off and handed to the office until the end of the school day. The office will keep a log and monitor the return of personal devices to its owner.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone, phoned and monitored by a member of staff.
- Any personal devices taken on out of school trips should be handed to a member of staff.
- Parents will be informed should a child bring a personal device to school and not hand it in to the office.
- Any personal devices found in school that have not been handed into the office will be removed and taken immediately to the school office. Parents will be informed and the device may be collected at the end of the school day.

9.7 Visitors Use of Personal Devices and Mobile Phones

- Visitors, parents/carers to the school must use mobile phones and personal devices in accordance with the school acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers is not allowed around the children.
- Visitors cannot use personal devices to photograph or video children.
- Visitors and parents/carers will be unable to access the school network.
- Guest Wi-Fi logins will be provided to visitors to the school who require Internet access on their personal devices. Codes will be given that expire after 24 hours.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

10. Related Policies

Child Protection and Safeguarding
Behaviour and Relationships
Relationship, Sex and Health Education
Staff Code of Conduct
Data Protection (GDPR
Whistleblowing
Staff Disciplinary Policy
Artificial Intelligence Policy

Online Safety at Yarborough Academy



APPENDIX

EYFS and Key Stage 1 Pupils and Special Grown-Ups Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS, REMOTE EDUCATION AND INTERNET AGREEMENT FOR PUPILS AND SPECIAL GROWN-UPS

Name of pupil:……

When I use the school's ICT systems (like iPads) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school iPads for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work as directed to do so by my teacher
- Check with my teacher before I print anything
- Log off or shut down apps when I have finished using them

I agree that the school will monitor my use of ICT systems, email, Google Suite and internet and that there will be consequences if I don't follow the rules.

Dear Special Grown-Ups

The use of IT including the internet, e-mail, mobile, social networking, remote and online learning etc. has become a crucial part of learning and we want all pupils to be safe and responsible while using these valuable resources. We may also use remote learning tools to continue educating children at home.

Please sign to agree with the following statements:

*We have discussed this acceptable user agreement and …….....(child's name) agrees to follow the Online Safety rules and to support the safe use of IT at Yarborough Academy.
*As a parent, I am aware of the benefits as well as risks of online learning and will help my child to stay safe and follow the rules.
*We will contact the school if any issues or concerns arise in terms of internet use/online learning/online safety. The staff responsible for this are Miss Howard and Mr Pickerden.

Signed (Special Grown-Up): **(on behalf of myself and my child)**	**Date:**

APPENDIX

Key Stage 2 Pupils and Special Grown-Ups Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR PUPILS AND SPECIAL GROWN-UPS

Name of pupil:……

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like iPads) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Only use my class Google account or individual school Google account to access sites as directed by my teacher. I know that this means whilst I am in school and when I am at home
- Only use my individual school Google account for remote learning purposes as directed by my teacher. I will not use it for personal use.
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or trusted adult) immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer/iPad/app when I'm finished working on it
- Only open/delete my own files
- Be responsible for my own behaviour when using IT because I know that these rules are to keep me safe.
- Understand that my usage is monitored by the school.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Bring any devices from home. If I bring a phone, I will hand it to the Office and collect it at the end of the day
- Use any inappropriate language when communicating online, including in emails
- Log in to any form of ICT or app using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I know that my use of IT can be checked and that my special grown-up will be contacted if a member of school staff is concerned about my online safety.

I agree that my image may be used on the school website

I understand that most social networking sites have a minimum age of 16 years old and will tell my special grown-up if I have a social network account.

I agree that the school will monitor my use of ICT systems, email, Google Suite and internet and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**
Dear special grown-up The use of IT including the internet, e-mail, mobile, social networking, remote and online learning etc. has become a crucial part of learning and we want all pupils to be safe and responsible while using these valuable resources. Please discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Miss Howard or Mr Pickerden. We have discussed this and ……..…..(child's name) agrees to follow the Online Safety rules and to support the safe use of IT at Yarborough Academy. As a parent, I am aware of the benefits as well as risks of online learning and will help my child to stay safe and follow the rules.	
Signed (special grown-up):	**Date:**

APPENDIX

Staff Code of Conduct for ICT / Computing Acceptable Use Agreement

- I understand that it is a criminal offence to knowingly use a school ICT/Computing system for a purpose not permitted by its owner.
- I appreciate that ICT/Computing includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT/Computing use may also include personal devices when used for school business, in and out of school.
- I understand that school information systems are intended for educational use and not to be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email is monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that personal data is stored securely using the school's VPN or Google Drive and I will not copy personal data to my own devices.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Online Safety policy and staff code of conduct.
- Personal equipment must not be used to educate or photograph the children without prior consent from the headteacher.
- I will only use personal devices to take photographs of children when no wireless connections are available. I will remove any image from my device immediately after they have been transferred as necessary.
- Appropriate use of mobile phones is acceptable on educational visits to ensure the safety of the children.
- I will respect copyright, data protection and intellectual property rights.
- I will take full responsibility for any academy equipment and treat it as though it were my own.
- I understand that outside of school hours, academy equipment is not covered by the school's insurance policy for loss, theft or damage. I will report any incidents to the Online Safety lead and I may incur a cost.
- I will report any incidents of concern regarding children's safety via the school's reporting system (CPOMS) and to the relevant members of staff in line with the safeguarding and online safety policy.
- I will ensure that electronic communications with pupils and parents are using the official school systems, compatible with my professional role, written in a professional tone and manner, and written so that they cannot be misunderstood or misinterpreted.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will monitor pupil's use of mobile technology and ensure all use is educational.
- I understand that any school login must have a strong password that I will change 3 times a year
- I will report any pupils' inappropriate use of technology e.g. cyberbullying, accessing social media etc. as per the online safety policy.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute and follow the expectations in the Online Safety policy.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal social media links, to pupils or families.
- I will immediately report any illegal, inappropriate, or harmful material or incident.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I will ensure that I use a personal Apple ID for my own devices and a school Apple ID (my school email address) for my school device.
- I will ensure that photo sharing is turned off between school and personal devices.
- I will not use personal electronic devices (including smart watches) in public areas of the academy during school hours, except in the staff room.
- I will ensure appropriate use of Guest Wi-Fi, in line with my professional role and responsibilities in school.
- Academy equipment that is used outside academy premises, for example laptops/macbooks/ipads, should be in school every day and should be returned to the academy when the employee leaves employment or if requested to do so by the Headteacher.
- I will use only closed AI school approved resources (such as Teachmate, not Chat GPT).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police

Name:	**Date:**
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety and security of the ICT systems and other users. I recognise the value and use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will educate the young people in my care on the safe use of ICT and embed online safety in my work with young people. **Members of staff should consult the school's Online Safety policy and Code of Conduct for further information and clarification. I will return school equipment to the academy when requested to do so by the Headteacher.**	
Signed:	