Hunslet Moor Primary School
Online Safety Policy

To be adopted by Hunslet Moor Primary School Governing Body
September 2026

To be reviewed by Governors September 2028

1. INTRODUCTION

1.1 Hunslet Moor Primary School recognises that ICT (Information and Communication Technology), the internet, and social networking are important tools for aiding teaching and learning, providing opportunities for research and investigation and create a forum for the communication of ideas. Technology enriches the curriculum, enhances the learning experience of students and supports creativity and independent thinking.

1.2 The use of ICT to interact socially and share ideas can benefit staff, students and parents/carers; however, it is important that the use of the internet, tablets, e-readers, gaming systems and mobile phones is seen as a significant responsibility for students, staff and parents/carers that must be used appropriately.

1.3 It is essential that all staff, students and parents/carers are alert to online safety and the possible risks when using the internet and chat rooms, social networking, gaming and mobile phones with internet access. It is also important that staff, students and parents/carers are aware of the importance of responsible conduct online.

1.4 We know that some adults and young people will misuse mobile phones, the internet, chat rooms and social networks to harm children and young people. The harm might range from sending abusive texts and emails, to harassment and stalking behaviour and coercing children and young people to engage in sexually harmful conversations or actions online; such as webcam filming, sending explicit photographs, or arranging face-to-face meetings. This can also lead to blackmail, sharing of inappropriate images, CSE (Child Sexual Exploitation) and sexual abuse.

1.5 Staff members have a responsibility in accordance with 'Keeping Children Safe in Education' (DfE, 2026) to safeguard students and report abuse immediately to designated staff members. Every member of staff will attend child protection training which outlines forms of abuse, and includes the indicators and signs of CSE.

1.6 Staff members have a responsibility in accordance with 'Keeping Children Safe in Education' (DfE, 2026) to support children in understanding the risks linked to Artificial Intelligence (AI) generated material online.

1.7 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers Hunslet Moor to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. 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.

1.8 All staff members have a ‘duty of care’ to ensure that students are educated about online safety, know how to reduce risk of harm and stay safe, are able to report abuse and know who to talk to about any concerns around the use of this technology. There is also a duty to ensure that staff conduct does not bring into question their suitability to work with students.

1.9 Children who have been subject to abuse (including child on child abuse) should know they will be taken seriously, be supported and kept safe. They should not be made to feel ashamed for making a report or that they are creating a problem.

1.10 When used in the correct manner this technology can give students, staff and parents/carers many opportunities for personal development and there needs to be a balance between controlling access to the internet and technology and allowing students the freedom to explore and use these tools to their full potential.

1.11 The computing subject leader along with SLT will ensure the development of an online safety policy, oversee the procedures outlined in the policy and provide advice for staff and students about e-safety.

1.12 A school Governor will have the responsibility for online safety to implement the online safety policy and ensure it is disseminated to staff.

2. AIMS OF ONLINE SAFETY POLICY

2.1 This policy aims to outline procedures for the use of ICT and technology by staff and students at Hunslet Moor Primary School.

2.2 The policy will define the code of conduct for staff when online and when using related technologies, and provide online safety guidelines.

2.3 The policy aims to raise awareness of good online safety practice focused upon the value and benefits of using ICT and related technologies, whilst being mindful of the possible risks and dangers involved.

2.4 This policy is available on the school website for access by parents/carers, staff and students.

2.5 Throughout this policy children and young people are referenced as students. For the purpose of safeguarding and child protection. The term students include all children, young people and young adults at risk who professionals may come into contact with, as part of their role.

3. PROFESSIONAL EXPECTATIONS

3.1 The use of computer systems without permission or for purposes not agreed could constitute a criminal offence under the Computer Misuse Act 1990.

3.2 Staff members are adults and as such should act responsibly and with an awareness of the consequences of their actions. Staff members must act with the best interests of students at all times.

3.3 Staff who are provided with a laptop or tablet by the school must use this only for academic purposes, these remain the property of the school and open to scrutiny by Senior Leaders.

3.4 All staff members are responsible for their personal use of social media, networks and electronic device and are expected to ensure that any use of such technologies does not breach the Safer Working Practice or undermine the reputation of the school or Local Authority.

3.5 Staff are personally responsible for the security and privacy settings when using social media and networks and failing to ensure that privacy settings are secure could lead to a disciplinary process if the content breaches professional expectations.

3.6 Staff must ensure that their use of ICT and social media is professional at all times, even if this is outside of the school day, and that behaviour which breaches the school's code of conduct could lead to disciplinary action.

3.7 All contact made with students must be made through appropriate channels, such as Class Dojo or Google Classroom, and should be made within clear and transparent professional boundaries and only made with regard to matters regarding the school.

3.8 Safe and professional behaviour of staff online will be discussed at staff induction training.

3.9 Appropriate computer usage

3.9.1 Staff members are expected to use computers in lessons only for teaching and learning.

3.9.2 Staff should ensure that students are unable to access activities and information on the computers that is not relevant to teaching and learning and the lesson.

3.9.3 Staff should log off or lock their computer when not in use to protect confidential and personal information.

3.9.4 Only IT Technicians from Primary ICT should move computer equipment, unplug cables or remove screws or covers from equipment and upload/download or copy programs and change, or attempt to change the configuration of any computer.

3.9.5 Students should not use computers in classrooms without permission or without a member of staff being present, specifically at non-contact times to ensure that staff members are able to supervise online access and secure equipment.

3.9.6 Any misuse or damage to computers in classrooms should be reported to technicians immediately.

3.9.7 Staff may be liable to pay for any damage caused by themselves to school equipment intentionally or accidentally. Each circumstance will be dealt with individually.

3.9.8 When taking computers offsite staff should ensure they are stored safely and securely at all times.

3.10 Social media and networks

3.10.1 Students should not be added as friends and staff must not respond to friend requests. If a member of staff suspects that an existing friend is a student or a student is using another name to befriend the member of staff the friendship should be ended and this should be reported to SLT.

3.10.2 If a member of staff coincidently has a contact established with an ex-student, parent/carer or student the member of staff must use their judgment and regulate this contact. If a student, ex-student or parent/carer persistently attempts to befriend a member of staff this should be disclosed to SLT.

3.10.3 The use of personal social networking activity is at the discretion of the individual, however the professional responsibilities of the individual need to be considered in all postings on these sites.

3.10.4 It is important to ensure that your personal information is secure and that high strength passwords are used and that profile settings are restricted. It is advisable to log out of social networking sites when not in use as a security precaution.

3.10.5 Staff must be aware of how to set privacy settings on their profile (refer to Annex A) and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their profile privacy settings.

3.10.6 Professionals should consider what information they use for their profile, for example the photograph and the amount of personal information that is displayed. Profiles should not identify your employer or place of work.

3.10.7 Staff should not publish their school email address on a personal social networking site, or use this address as part of your login/registration on a personal site.

3.10.8 All postings on social media and networks should be considered to be in the public domain so staff members should consider this when making decisions about the content of social media activity.

3.10.9 Any material which is posted on social media and networks which is considered to bring the School into disrepute or is considered to put students or staff at risk of harm will be dealt with in a formal procedure.

3.10.10 Staff members should not make reference online to any students, parents/carers, colleagues or to any work related issue. This also includes posting photographs or videos online which identify your place of work, or any students and parents/carers.

3.10.11 While access to social media sites through the School network is blocked to employees, accessing the internet through mobile phones and other mobile devices is restricted to break times only. Mobile phones or other mobile devices are not allowed to be used in 'No Mobile Phone Zones', these are clearly identified by signs in the area. It is strongly advised that the posting of social media content is kept outside of school hours.

3.11 Social Media advice

3.11.1 Social Media has enabled families and friends to stay in contact and have lessened geographical divides, it is important, however that this media is used appropriately. To ensure that staff are safe and protected as professionals:

- Keep your profile picture post modest. Remember students can still search for you and see your picture without being your friend.
- Create your photo albums with privacy settings so 'only your friends' can see them.
- Reject all friend requests from students. You do not need to report this unless it becomes a recurring problem. People are not notified when you reject their friend request.
- Use social media privacy settings to limit who can see your full profile. Set it so that only friends can see everything like your pictures, your wall, and your personal and contact information.
- Use limited public information about yourself on your profile. For example address, email, date of birth, contact telephone numbers do not need to be shown to everyone, they can be privately messaged if needed.
- Do not use your school email address as your email contact.
- Do report any threats of violence or other inappropriate posts/images to Facebook or to the relevant authorities, such as CEOP (Child Exploitation and Online Protection centre) or the police.
- Customise your privacy settings. Limit what people can see when you 'poke' or message them before you have added them as a friend. The default setting allows people who are not friends whom you 'poke' or message to see your entire profile.
- Don't ever announce on your wall if you're going away. Many cases of burglaries are supported through the use of these disclosures on Social Media.

3.12 The use of mobile phones and personal devices

3.12.1 Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the school curriculum or for a professional capacity the school equipment will be used.

3.12.2 The use of personal equipment in school can only be authorised by the Senior Leadership Team in order to comply with safer working practice guidance, data protection and school policies.

3.12.3 Any breach of the school Online Safety Policy may result in disciplinary action against that member of staff.

3.13 Inappropriate material

3.13.1 In law there is a distinct difference between material that is inappropriate and that which is illegal, however accessing of inappropriate material is a significant concern with regards to safeguarding. Staff should be aware that the accessing of illegal material will lead to a case investigation, allegations management procedures, a possible criminal investigation, prosecution and barring, even if there is no criminal prosecution.

3.14 Illegal material

3.14.1 It is illegal to make, possess or distribute indecent images of a person under the age of 18 and viewing these images online may constitute possession even if they are not saved. Accessing indecent images of children or students on the internet or making, storing or distributing such images of students or children is illegal and if proven could lead to criminal investigation and the individual being barred from working with students.

3.15 Materials which incite hate, harm or harassment

3.15.1 There are a range of offences in relation to incitement of hatred on the basis of ethnicity, gender, sexual orientation, gender identity religion and beliefs and offences concerning harassment and threatening behaviour which include cyber bullying, whether this is carried out on a mobile phone, social networking or through email. It is an offence in law to send indecent, offensive harassing or threatening messages which cause the recipient distress. Hate crime is a matter for the police and they must be called if a student or member of staff is victim to a hate crime.

3.14 Confidentiality and Data

3.14.1 Members of staff have access to confidential information about students, other staff and parents/carers in order to undertake their daily duties, this may sometimes include highly sensitive information. This information must not be shared outside of school or with external parties unless a student is at risk of harm or significant harm or there is an agreed multi-agency plan around a family and student.

3.14.2 Confidential information should only be stored on school systems and email should never be used to transfer sensitive and confidential information. In such cases, sensitive and confidential information should only be shared using mail express or other secure methods of communication such as CPOMs.

3.15 Cyberbullying

3.15.1 Cyberbullying, bullying, harassment, defamatory comments, offensive correspondence and hate incidents within and outside Hunslet Moor Primary School will not be tolerated and any member of staff found to be behaving in this manner towards colleagues will be dealt with in accordance with the Bullying and Harassment Policy and in specific circumstances will be considered as a criminal offence.

3.15.2 If any member of staff is a victim of this behaviour they must follow the Whistleblowing Policy and report this behaviour as soon as possible to their line manager or SLT. The victim will be offered support and this will be fully investigated

and the Bullying and Harassment Policy followed, a referral may be made to the appropriate authorities if deemed appropriate.

4. POLICY AND GUIDANCE FOR THE SAFE USE OF STUDENT PHOTOGRAPHS

4.1 Photographs, images of students work and recorded images are part of daily school life and enhance the learning experience and environment for our students, parents/carers and staff members. They are used to showcase the talents and work of our students, express our pride for our school and celebrate the talents of the student body. We therefore acknowledge the importance of having safety precautions in place to prevent the misuse of such material.

4.2 Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without parental permission. On admission to Hunslet Moor Primary School, parents/carers will be asked to sign a photography consent form. The School does this so as to prevent repeatedly asking parents/carers for permission over the academic year.

4.3 Images of students must not be displayed or distributed, for example in a newsletter or website, without parental permission.

4.4 Permissions can be found on the child's individual SIMs record.

4.5 Using photographs of students

4.5.1 Photographs and video images must be created with School equipment only. No members of staff should use personal devices to record or store images of students.

4.5.2 It is important that published images do not identify students or put them at risk of being identified. School is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions unless permission has been given. Only images created by or for school will be used in public and students may not be approached or photographed while in School or doing School activities without the School's permission.

4.5.3 Electronic and paper images of students will be stored securely and the names of stored photographic files will not identify the student.

4.5.4 Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).

4.5.5 When images are used for public documents, including in newspapers, full names will not be published alongside images of the student. Groups may be referred to collectively by year group or form name.

4.5.6 Events recorded by family members of the students such as School plays or sports days must be for personal use and only at the discretion of the School. Parents should only take photos of their own child.

4.5.7 Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

4.5.8 Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students.

4.5.9 Child Protection Designated Officers are aware of students who need protection

from their image being used and will ensure that staff members are made aware of students who cannot have their image published in any form.

5. CONSEQUENCES OF INAPPROPRIATE ACTION BY STAFF MEMBERS

5.1 Hunslet Moor Primary School may exercise the right to monitor the use of the school computer systems, including access to websites, the interception of email and the deletion of inappropriate materials, without the consent of the staff member should inappropriate actions or behaviour occur.

6. TEACHING AND LEARNING THROUGH ICT

6.1 Online safety is integrated into the Hunslet Moor curriculum in every circumstance where the internet or technology is being used.

6.2 Students will be made aware about the possible risks and dangers that they might encounter when using ICT, the internet, mobile phones, gaming stations and personal devices through computing lessons, implicitly throughout the curriculum and in PSHE. This will include understanding the importance of keeping personal information private and staying safe online.

6.3 The internet is used in school to raise educational standards, promote student achievement, support the professional standards of the work of staff members and to enhance the school's management functions. It is the responsibility of every staff member to equip students with the necessary ICT skills, transferable knowledge and awareness to enable them to make outstanding progress and fulfil their potential.

6.4 Students will have access to ICT and online safety information as part of their Computing curriculum, and/or via access to the ICT where they can access a number of teaching and learning resources.

6.5 ICT can be used to give students the freedom to be creative and the opportunity to explore the world and its differing cultures from within a classroom. It can be used as a tool for social inclusion, in class and online and to provide individualised access to learning.

6.6 For staff, ICT can aid professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies. It can allow professionals to access professional support through networks and associations. It is a communication tool which gives professionals the ability to mark and assess student work and provide immediate feedback to students and parents/carers. It is also an administrative instrument used for class management, attendance records, schedule, and assessment tracking.

6.7 Engagement with parents/carers is important and integral to the work of staff and ICT gives parents/carers access to the school website pages with a wide variety of educational resources to help support students with homework and to aid learning from home.

6.8 Learning to evaluate internet content

6.8.1 There is a multitude of information available online and it is important that students learn how to evaluate internet content for accuracy and intent. Students are taught to become digitally literate across the whole curriculum and are encouraged to be critically aware of materials they read, and how to validate information before accepting it as accurate. Students will be taught to understand the bias of web authors and separate fact from fiction. Students learn how to use age-appropriate tools to search for information online, how to acknowledge the source of information used and to respect copyright.

6.8.2 Hunslet Moor Primary School will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL must be reported to SLT and Primary ICT.

6.8.3 Regular software and broadband checks will take place to ensure that filtering services are working effectively.

7. SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

7.1 It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

7.2 Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and possible long term implications of this information being in the public domain.

7.3 Students are educated on the dangers of social networking sites and how to use them in safe and productive ways, whilst also reminded of the legal age of different social media sites and apps.

7.4 Official school blogs created by staff or students, will be password-protected and will be incorporated on the school website with the prior approval of SLT.

7.5 The school Twitter page will be used solely as an advertisement and platform to show case the excellent work and outstanding contributions the children have made to school life.

7.6 Twitter consent will appear on a child's individual SIMs page and permission will be gained when a child joins Hunslet Moor Primary school.

8. SPECIAL EDUCATIONAL NEEDS AND DISABILITIES (SEND)

8.1 ICT can be a positive tool for students with SEND and access to the internet and ICT is a vital link for communication with the outside world and other students, which can allow every student to have access to information, communicate with others and develop ideas and research independently.

9. MONITORING

9.1 School will take any issues identified by staff, students and parents/carers, regarding any breach of social media sites seriously and this will be investigated and dealt with by the Senior Leadership Team.

10. MOBILE PHONES AND PERSONAL DEVICES

10.1 Hunslet Moor will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.

10.2 Images or files should not be sent between mobile phones in school and mobile phones can be confiscated by a member of staff, and the device can be searched by a member of the Senior Leadership Team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

10.3 Hunslet Moor is committed to maintaining a mobile free learning environment. Pupils in Years 5 and 6 may bring a mobile phone to school where their parent/carer considers it necessary, for example, if they walk to or from school independently. Phones must be switched off on arrival, handed to a member of staff and stored securely in the Safeguarding Office until dismissal. Pupils must not use their mobile phone until they have left the school premises.

10.4 Pupils must not use their mobile phones during the school day unless directed by a member of staff in exceptional circumstances. Failure to follow these expectations will be dealt with in accordance with the school's Behaviour Policy.

10.5 Any use of a mobile phone that raises a safeguarding concern will be managed in accordance with the school's safeguarding procedures, logged on CPOMs and referred to the Designated Safeguarding Lead.

11. ARTIFICIAL INTELLIGENCE (AI) GENERATED MATERIAL

11.1 Hunslet Moor recognises that artificial intelligence (AI), including generative AI, is increasingly accessible to children and can create text, images, audio and video that may appear realistic but may be inaccurate, misleading or harmful.

11.2 In line with Keeping Children Safe in Education 2026, the school recognises the safeguarding risks associated with AI-generated content, including misinformation and disinformation, inappropriate or harmful material, manipulation, bullying and the creation or sharing of AI-generated images, including deepfakes.

11.3 Pupils will be taught age-appropriate strategies to question, check and critically evaluate AI-generated content and to understand that not everything created or presented by AI is true or safe. This will take place through their online safety lessons, PSHE lessons and the Personal Development programme.

11.4 Pupils will be encouraged to report anything that makes them feel uncomfortable, worried or unsafe.

11.5 Hunslet Moor ensures that any AI tools used by pupils or staff are age-appropriate, approved by the school and used in accordance with safeguarding, filtering and monitoring, data protection and acceptable use requirements.

11.6 Personal or sensitive information about pupils or staff must not be entered into AI tools unless specifically authorised and appropriately protected.

11.7 Any safeguarding concern involving AI-generated content will be reported and managed through the school's established safeguarding procedures.

12. CYBER-BULLYING

12.1 Cyberbullying is defined as bullying that takes place using electronic technology.

Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and distributing embarrassing pictures, videos, websites, or fake profiles.

12.2 Cyber bullying by students and staff will not be tolerated and will be treated as seriously as any other type of bullying.

12.3 If a member of staff is aware of a bullying incident they must take this seriously, act as quickly as possible to establish the facts and report the incident to the appropriate member of staff. These members of staff will investigate the matter fully, provide support for the victim, try to act restoratively and apply sanctions when necessary.

13. PUBLISHED CONTENT AND THE SCHOOL WEBSITE

13.1 The school website is a tool for communicating the school's ethos, academic pride and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with school news and events, celebrating personal achievements, and promoting school projects, events and extra- curricular activities.

13.2 The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school's students and staff, copyrights and privacy policies. No personal information about students or staff will be published, and details for contacting the school will be for the School office only.

14. PROTECTING PERSONAL DATA

14.1 Hunslet Moor Primary School believes that protecting the privacy of our staff, students and parents/carers and regulating their safety through data management, control and evaluation is vital.

14.2 School collects personal data from students, parents/carers, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

14.3 School takes responsibility for ensuring that any data collected is used correctly and only as is necessary, and will keep parents/carers fully informed of how the data is collected, what is collected, and how it is used.

14.4 National Curriculum results, attendance, assessment data, registration records, SEND data, and any relevant medical information are examples of the type of data that Hunslet Moor Primary School will capture. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of students to ensure that they receive an outstanding education and to respond to the changing needs of students.

14.5 In line with the Data Protection Act 1998, we will follow the principles of good practice when processing data. We will ensure that data is fairly and lawfully processed and only for limited purposes. School will ensure that all data processed is adequate, relevant, accurate and not excessive. Data will only be kept for the period of time that is necessary. It will be processed in accordance with the data subject's rights and will always be secure and not transferred to other countries without adequate protection.

14.6 There may be circumstances where School is required either by law or in the best

interests of our students or staff to pass information onto different authorities; for example, our Local Authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

15. REMOTE LEARNING

15.1 Devices purchased for the purpose of remote learning will be purchased through DfE certified channels. Hunslet Moor will ensure that devices have appropriate filtering and security software meaning children are protected from accessing inappropriate materials.

15.2 Remote learning will be delivered through a safe and secure platform and will ensure that all pupils and staff are safeguarded effectively.

15.3 Parents and Carers will be asked to sign documentation to state they understand the purpose of the technology and that it shall be used appropriately and safely by the child under supervision of an appropriate adult.

15.4 The need/decision for a child to access remote learning will sit with the Headteacher and will be on a case by case basis.