

THE EDWARD RICHARDSON PRIMARY SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Date of last review	Autumn 2024
Term next due for update	Autumn 2026
Member of staff responsible for this update	Headteacher
Online Safety Leader	Headteacher
IT Technical Support	Education Lincs
Governor responsible for this update	Safeguarding Governor
Requirement	Non-statutory

This policy has been created with a school emphasis using guidance from Lincolnshire Safeguarding Children's Board. Throughout the policy, it addresses the four main areas of online safety – content, contact, conduct and commerce.

Use of the Internet - the internet is provided to help pupils with learning activities such as research, online activities and online educational games/apps. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. If a pupil is unsure, or comes across anything they feel is inappropriate, they are taught to inform the nearest adult in school as soon as possible.

Role of the headteacher

Reporting to the governing body, the headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to the named member of staff above. The headteacher will ensure that:

- Online Safety training throughout the school is planned, up to date and appropriate to the recipient;
- All Online Safety incidents are dealt with promptly and appropriately.

Role of the Online Safety Leader

The Online Safety Leader will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the headteacher;
- Advise the headteacher and governing body on all Online Safety matters (if not headteacher);
- Engage with parents and the school community on Online Safety matters at school and/or at home;
- Liaise with the local authority, IT technical support and other agencies as required;
- Retain responsibility for the Online Safety risk assessment;
- Ensure any technical Online Safety measures in school (e.g. Internet monitoring and filtering software) are fit for purpose through liaison with the local authority and/or IT technical support.

Role of the IT technical support staff

Technical support staff are responsible for ensuring that:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices;
- Operating system updates are regularly monitored, and devices updated as appropriate;
- Any Online Safety technical solutions such as Internet filtering are operating correctly;
- Filtering levels are applied appropriately according to the user (staff and pupils);
- Passwords are applied correctly to all users regardless of age;
- The IT System Administrator password(s) is/are changed on a regular basis.

Role of all other staff (in both a paid and unpaid capacity)

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the headteacher;
- Any Online Safety incident is reported to the Online Safety Leader or in his/her absence to the headteacher.

Risk assessment of potential issues/dangers

The Online Safety Leader will ensure that the risk assessment is kept up-to-date in line with technological developments within the school (located at the end of this policy). The risk assessment will be shared with all staff members and the school's IT technical support provider.

In the event of staff/pupils accidentally accessing online material that they deem to be inappropriate/offensive, it will be reported to the Online Safety Leader or, in their absence, to the headteacher.

Protection against extremism/radicalisation

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the Internet as a means of either inciting violence against specific groups or providing information on carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Appropriate filtering is in place and will be reviewed whenever there is an incident of pupils accessing websites advocating extremism;
- The Online Safety Leader will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school or its pupils;
- A referral will be made to the police whereby a pupil is deeply involved in the extremist narrative and there is evidence that their parents are involved in advocating extremist violence.

Child on child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online child on child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Supporting pupils' mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the

internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online Safety training for staff

As part of our Safeguarding training pathway, all staff undertake training in Online Safety. However, in addition to this, all staff will receive annual face-to-face online safety training from an online safety specialist.

Social Networking

1 Staff and governors using social networking websites and/or apps

- 1.1 Staff are within their rights to use social networking websites and we are not, nor would not want to be, in a position to prevent staff from using them. However, we do ask that staff adhere to the following aspects of our policy:
- 1.2 Under no circumstances should pupils or ex-pupils under the age of 13 be befriended on a social networking website. If a child requests the befriending of a staff member, their parents should be informed.
- 1.3 In the event that a parent makes contact with a staff member through a social networking website, the staff member must use extreme caution, and it is recommended that they provide the school email address as a point of contact for professional purposes. In the event of communicating with a parent or adult associated with a child who attends the school, no comments should be made about pupils, staff or parents.
- 1.4 Any statements or status remarks published on personal social media, in any capacity, should not contain any comments about the school, staff, parents or pupils – unless it is a direct share of a post from the school's own social media account.
- 1.5 All views expressed by staff members on social networking websites are their personal views and are in no way endorsed, nor supported, by the school. Staff should, however, always assume that anything posted on social media would be attributed to them as a professional – particularly if made public.
- 1.6 School employees and volunteers must not identify themselves as associated with the school in any way, unless expressly authorised by the headteacher. Authority to use official school social media will be given to individual members of staff by the headteacher.

2 Pupils using/accessing social networking websites and/or apps

- 2.1 Under no circumstances should a child access social networking websites in school unless it is for a purpose instigated by the child's teacher. The school network system prohibits pupils from accessing these websites but the bypassing of the system or accessing through a mobile phone is strictly prohibited.
- 2.2 If any reports are received of pupils making inappropriate comments about staff or other pupils, hard copies will be obtained, and the child will be reported immediately (to the website host) to have their account terminated. The parents/carers of the child will also be notified, and this could result in further action. If the comment is about a member of staff a referral may be made to the county's legal services.

3 Parents using social networking websites and/or apps

- 3.1 If hard copies of inappropriate comments about members of staff, pupils within the school or school decisions are received, the matter may be referred to the county's legal services and subsequent action will follow.
- 3.2 School visits: parents must not, under any circumstances, access social networking accounts whilst assisting staff members. They must also ensure that they do not take photographs/videos on a personal device. If there is evidence to prove that this has happened, then the parent will no longer be used as a helper on subsequent visits. If this is considered a GDPR breach, it will be reported in accordance with our GDPR policy.
- 3.4 Staff who are also parents or carers of pupils at the school must communicate about their own child through the same official channels as all other parents. Personal messaging services (eg: text message, WhatsApp or social media messaging) must not be used to raise questions, concerns or requests relating to their child with other members of staff. This ensures fairness, maintains professional boundaries, safeguards all parties and ensures an appropriate record of communication.

Acceptable Use

1 Aim

- 1.1 The aim of this section of the policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet and technological resources in a safe and effective manner.

2 General

- 2.1 Pupils will be supervised by an adult whilst using the Internet. Online Safety is taught as part of our Computing curriculum.
- 2.2 Filtering systems (two-level) are used by our Internet Service Provider in order to minimise the risk of exposure to inappropriate material.
- 2.3 Downloading of non-approved software is prohibited, and software can only be downloaded and deployed by our IT provider.
- 2.4 Virus protection is present and maintained on all relevant devices.
- 2.5 Staff will require permission from the headteacher to use portable storage media (USB memory sticks, discs, SD cards, etc) on any school device. Any such device containing sensitive or pupil data must be encrypted in order to prevent GDPR breaches.
- 2.6 Staff should keep personal passwords private. Under no circumstances should a personal password be shared with a staff member, pupil or IT technical support staff. If staff feel that a password has been compromised, they should report this to the headteacher or Online Safety Leader immediately.
- 2.7 Passwords to whole-school resources can be shared so long as password access does not lead to any pupil information other than name and year group (eg: TTRockstars).

3 World Wide Web

- 3.1 School staff and pupils will not intentionally attempt to access material deemed inappropriate or material that is blocked by filtering systems.
- 3.2 Pupils will not copy information from other sources without acknowledging and citing the original source (copyright infringement).
- 3.3 Pupils will never disclose or publicise personal information.
- 3.4 Web filtering does not allow pupils access to commerce.

4 Email/Google Meet/Microsoft Teams

- 4.1 School staff and pupils will only use approved email and online meeting accounts whilst on site.
- 4.2 School staff and pupils will not send material that is illegal, obscene, defamatory or material that is intended to annoy or intimidate another person.
- 4.3 Although we do not want communication to come across as 'cold', all communication will be kept professional in content. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

5 Personal devices

- 5.1 Pupils may only bring personal devices into school with permission from their teacher.
- 5.2 Pupils' personal devices will not be allowed to access Internet in school unless under exceptional circumstances (agreed by the Online Safety Leader or headteacher).

6 Portable devices/tablets

- 6.1 All iPads are managed by the school's IT provider and these are never taken off-site by staff or pupils.
- 6.2 All laptops are managed by the school's IT provider and these may be taken off-site by teachers due to the relevant levels of encryption.

7 Mobile phones/smart devices

- 7.1 School staff, volunteers, parents and contractors are allowed to bring in personal mobile phones/smart devices for their own use. Staff, volunteers, parents and contractors should use their personal mobile phones/smart devices with caution. The responsible use of personal mobile phones and devices is based on an agreement of trust that; *during times when children are on the school premises, phones must be kept on silent and only used for an agreed purpose as outlined in the Staff Use of Mobile Phone*

Policy (ie: Two-factor authentication, school calendar access, etc). Staff, volunteers, parents and contractors may only make and receive calls out of school hours or in an emergency in the staff room.

- 7.2 Users bringing personal mobile phones/smart devices into school must ensure that there is no inappropriate or illegal content on the device – even if this is not immediately accessible or visible.
- 7.3 Staff, volunteers, parents and contractors will not use mobile devices to take images or videos of pupils, staff or any area of the school environment unless permission is granted by the headteacher. In these rare instances, the media will be removed (including from ‘recently deleted’ folders) before leaving the school site.

8 Examining electronic devices

- 8.1 The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
- Poses a risk to staff or pupils, and/or
 - Is identified in the school rules as a banned item for which a search can be carried out, and/or
 - Is evidence in relation to an offence
- 8.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from one of the school’s DSLs
 - Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
 - Seek the pupil’s co-operation
- 8.3 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so. When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
- Cause harm, and/or
 - Undermine the safe environment of the school or disrupt teaching, and/or
 - Commit an offence
- If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

Risk Assessment

*This is the product of the likelihood and the impact, and is categorised as below:

Risk	Area	Likelihood	Impact	Score*	Actions
Access to inappropriate content (staff)	Content	1	3	3	Appropriate Internet filtering is in place.
Access to inappropriate content (pupils)	Content	2	3	6	Appropriate Internet filtering is in place, set to a higher level than staff access. This is a two-level system: one at router level, the other via SENSO Cloud.
Misuse of copyright material (staff/pupils)	Conduct	2	2	4	Pupils are taught about copyright as part of the Online Safety element of the Computing curriculum. Staff aware of copyright guidelines.
Loss/theft of personal pupil data	Commerce	1	3	3	Encryption and security measures to be in place on all IT equipment as necessary.
Misuse/inappropriate activity on pupil iPads by pupils	Conduct	2	3	6	iPads set to pupil level of filtering with certain features/functions disabled and monitored via SENSO Cloud. Filtering at router level also in place. Pupils to be supervised when using iPads.
Theft of iPads	Conduct	2	1	2	iPads inside locked and alarmed building, and updated regularly with latest iOS. iPads protected with passcodes and GPS location discoverable via built-in software.
Falling victim to phishing or scam attempts, or DDoS attack	Commerce	1	3	3	Two-level filtering is in place. Staff are trained as part of annual online safety training regarding phishing and scams. Web application firewall (WAF) in place to block malicious HTTP traffic.
Theft of off-site school property (eg: laptops, iPads)	Conduct	2	3	6	Any off-site device to be encrypted and kept as safe as possible. Staff to ensure necessary due diligence.

medium risk

7 – 9 = high risk

1 – 3
= low
risk
4 – 6
=