

Task or Activity: Online Safety	Date assessment completed: 03/07/2026	Review Date: July 2027
Brief Details of Task or Activity Safety when accessing any online sources	Assessment completed by: C Riley & A Holmes	Signature: C Riley & A Holmes

What are the hazards?	Who might be harmed & how?	What are you already doing to control the hazard?	What further action or additional controls are required	Risk Rating	Action by who	Action by when	Date completed
Exposure to inappropriate sites or materials • Commercial ~ adverts, spam, sponsorship, personal info • Extremist ~ violent / hateful content • Sexual ~ pornographic or unwelcome sexual content • Values ~ bias, racist, misleading info or advice	Learners & Staff Accessing inappropriate or harmful materials at school or at home	◇ Providing an ICT Acceptable Use Policy for staff & learners, which is published on the website & signed by all new staff at induction ◇ Ensuring the school has effective monitoring & filtering procedures in place provided by Bolton SICT SLA ◇ Safeguarding learners online in & outside of school & assessing the needs of learners who may be at risk, ensuring all reported incidents of online bullying or online safety concerns are investigated & reported appropriately to the DSL & logged on CPOMS ◇ Providing comprehensive digital citizenship lessons, which are carefully planned, age-appropriate & progressive across the school through our computing & PSHE & relationships Education curriculum in line with the revised expectations for September 2026 ◇ Planning class assemblies & whole school events to promote online safety including participation in the Bolton SICT E-Safety competition annually, celebrating Safer Internet Day & providing online safety advice sessions for parents & carers, which highlight relevant current risks beyond the basic filtering & supervision guidance ◇ Distributing articles about online-safety in school newsletters/the website & providing links to resources to support parents & carers to understand & ensure their children use popular apps safely via the National Online Safety 'Wake Up Wednesday' campaign ◇ iPad contracts are in place & are signed by every child at the beginning of every year, highlighting the expectations for all school equipment & how it should be used safely ◇ Providing parents & carers with annual online safety workshops to ensure they are aware of current applications, developments in ICT equipment, how to ensure they have effective firewalls to protect their children at home & the importance of supervision ◇ Staff Safeguarding training (Level 1) provides detailed expectations to prevent radicalisation & the signs staff should be aware of; all staff are aware to report any concerns to the Designated Safeguarding Lead ◇ Annual online safety & CEOP training provided by Bolton ICT to all school staff to ensure they are aware of their roles & responsibilities regarding online safety & filtering & monitoring ◇ Implementation of Apple Classroom across the whole school as an extra layer of monitoring on the school iPads, this ensures that all iPads can be closely monitored & locked onto certain apps. ◇ Regular monitoring of Lightspeed from the DSL & DDSL & any incidents of online safety are reported to parents & Governors & logged on CPOMS	Organise Online Safety Parent & Carer Sessions Organise CEOP Training Launch Apple Classroom	D	Chloe Riley (DSL & KS2 DHT) & Nicola McGonagle (Computing Lead) Nicola McGonagle (Computing Lead) Chloe Riley (DSL & KS2 DHT) Nicola McGonagle (Computing Lead)	Online Safety Risk Assessment Review 03.07.26 Autumn 2026 Summer 2027 Autumn 2026	

What are the hazards?	Who might be harmed & how?	What are you already doing to control the hazard?	What further action or additional controls are required	Risk Rating	Action by who	Action by when	Date completed
Inappropriate online contact • Aggressive ~ being bullied, harassed or stalked • Sexual ~ harassment, meeting strangers, being groomed • Values ~ self-harm, unwelcome persuasions	Learners & Staff Risk of cyber-bullying or grooming	◇ Providing an Online Safety Policy for staff & learners, which is published on the website, signed by all new staff at induction & updated annually ◇ Ensuring learners & staff are aware of the procedures for reporting anything online that makes them feel uncomfortable (use of online reporting system ~ Zumos) ◇ Ensuring the school has effective monitoring & filtering procedures in place from the SICT ◇ Providing parents & carers with annual online safety workshops to ensure they are aware of current applications, developments in ICT equipment & how to ensure they have effective firewalls to protect their children at home ◇ Distributing articles about online-safety in school inclusion newsletters & on the website & providing links to resources to support parents & carers to understand & ensure their children use popular apps safely via the National Online Safety Wake Up Wednesday campaign ◇ Ensuring online safety is always high profile within the school through regular revisiting of how to stay safe online through our SMSC curriculum, assembly themes PHSE & Relationships Education & computing lessons ◇ Organising annual Healthy Relationships workshops for Y5 & Y6 learners (Fort Alice), which are inclusive of online safety ◇ Organising the NSPCC 'Speak Out, Stay Safe' assemblies with all learners in the summer term, which cover online safety & the potential dangers of communication online & how to identify unsafe requests & communication ◇ Implementation of Apple Classroom across the whole school as an extra layer of monitoring on the school iPads, this ensures that all iPads can be closely monitored & locked onto certain apps. ◇ Regular monitoring of Lightspeed from the DSL & DDSL & any incidents of online safety are reported to parents & Governors & logged on CPOMS ◇ iPad contracts are in place & are signed by every child at the beginning of every year. This highlights the expectations for all school equipment & how it should be used safely	Annual Review of Online Safety Policy (Governor Committee Meeting) Revised Digital Citizenship Lessons to be delivered as per the PSHE & Relationships Education Long Term Plan Check that all classes have discussed & signed their contracts	D	Chloe Riley (DSL & KS2 DHT) Nicola McGonagle & Zoe Cartridge (Computing Lead & PSHE & Relationships Lead) Nicola McGonagle (Computing Lead)	Updated May 2026, reviewed May 2027 Autumn 2026 Autumn 2026	

What are the hazards?	Who might be harmed & how?	What are you already doing to control the hazard?	What further action or additional controls are required	Risk Rating	Action by who	Action by when	Date completed
Inappropriate online behaviour • Commercial ~ Illegal downloading, hacking, gambling, financial scams, terrorism • Aggressive ~ being bullied, or harassing others • Sexual ~ peer harassment, creating & uploading inappropriate material • Values ~ providing misleading info or advice	Learners & Staff	◇ Providing an ICT Acceptable Use Policy for staff & pupils which is published on the website & signed by all new staff at induction ◇ Ensuring the school has effective monitoring & filtering procedures in place from the SICT ◇ Ensuring learners & staff are aware of the procedures for reporting anything online that makes them feel uncomfortable ◇ Providing comprehensive digital citizenship lessons which are carefully planned, age appropriate & progressive across the school through our computing & PSHE & relationships curriculum ◇ Planning class assemblies & whole school events to promote online safety including participation in the Bolton SICT E-Safety competition annually & celebrating Safer Internet Day ◇ Providing parents & carers with annual online safety workshops to ensure they are aware of current applications, developments in ICT equipment & how to ensure they have effective firewalls to protect their children at home ◇ Implementation of Apple Classroom across the whole school as an extra layer of monitoring on the school iPads. This ensures that all iPads can be closely monitored & locked onto certain apps. ◇ Regular monitoring of Lightspeed from the DSL & DDSL & any incidents of online safety are reported to parents & Governors & logged on CPOMS ◇ iPad contracts are in place & are signed by every child at the beginning of every year. This highlights the expectations for all school equipment & how it should be used safely	Ensure staff sign acceptable use agreement when using Guest Wifi (Log) Relaunch E-Safety Champions	D	C Riley (DSL) Sean Bailey (Personal Development Lead)	Autumn 2026 Autumn 2026	
Cyber & Information Security • Data Protection – data loss or compromised • Security Intrusion – information or access is compromised eg hack or virus/malware	Staff & learners Accounts being hacked Data being at risk of being shared Loss of access to the network drive or site closure	◇ Ensuring school has a safe & secure network & broadband connection at all times & reporting any issues immediately to SICT ◇ Providing secure remote access accounts for staff accessing the school system from home ◇ Ensuring all staff & learners are aware of & can access a clear reporting process for online-safety issues ◇ Providing all staff with data protection training via Global Policing ◇ Undertaking regular GDPR audits & reporting the outcomes & actions to governors termly ◇ Providing Individual staff & learner passwords to access all computers ◇ Saving all staff & learner documents onto the school network drive for security & protection ◇ Regularly updating the business continuity plan to ensure actions are in place in the event of a security intrusion or site closure ◇ Ensuring all members of staff follow the 'First Steps' & report concerns regarding a member of staff to the Head Teacher ◇ Recording any low-level concerns about a member of staff on 'Staff Safe'	GDPR Training to be updated by all staff	D	C Riley (DSL)	Autumn 2026	

What are the hazards?	Who might be harmed & how?	What are you already doing to control the hazard?	What further action or additional controls are required	Risk Rating	Action by who	Action by when	Date completed
Unsuitable use of online systems by a member of staff Safeguarding	Staff & learners Personal data sharing Inappropriate communication between staff & learners	◇ Providing online-safety policies (Online safety Policy & Acceptable Use Policy) which are read, understood, implemented & reviewed by staff, learners, parents & carers ◇ Providing staff with the Staff Code of Conduct & Mobile Phone Code of Conduct ◇ Implementing the Staff Capabilities procedure, where appropriate ◇ Providing all staff with CEOP training carried out by the local authority ◇ Maintaining an audit of all ICT & social media use including monitoring that of new members of staff as part of safer recruitment ◇ Regularly updating policies considering how all technology, online environments & mobile devices communicate, access social networks, music, videos & gaming sites, take photographs & record videos ◇ Ensuring all members of staff follow the 'First Steps' & report concerns regarding a member of staff to the Head Teacher ◇ Recording any low-level concerns about a member of staff on 'Staff Safe'	Staff Code of Conduct & Mobile Phone code of conduct to be shared with all staff Updated First Steps posters to be displayed around school	E	A Holmes (Head Teacher)	August 2026	August 2026
					C Riley (DSL)	Summer 2026	Summer 2026

CATEGORIES OF LIKELIHOOD

Highly Likely	Expected to happen/reoccur, possibly frequently.
Possible	Might happen/reoccur at some time depends on circumstances.
Unlikely	Not expected to happen/reoccur but possible in certain circumstances.
Highly Unlikely	Would only occur in very exceptional circumstances.

	Highly Likely	Possible	Unlikely	Very Unlikely
Catastrophic	A	A	B	E
Major	A	B	C	E
Significant	B	C	D	E
Minor	C	D	E	E
Negligible	E	E	E	E

CATEGORIES OF CONSEQUENCE SEVERITY

Highly Likely	Incident could result in <u>one or more fatalities</u> .
Possible	Major injury resulting in incapacity, hospitalisation >24 hours.
Unlikely	Injury requires attention of a Doctor or Hospital treatment or hospitalisation <24 hours.
Highly Unlikely	Small cut, bruise, abrasion, basic first aid treatment provided.

RISK CLASSIFICATIONS

A	Unacceptable risk , requires immediate attention. Work <u>should not be started or continued</u> until the level of risk has been reduced.
B	High risk , requires immediate attention. Control measures must be identified & put into place as soon as possible.
C	Medium risk , requires attention as soon as possible. The risk should be only be tolerated in the short term & only when further control measures are being planned & introduced, Timescales must be short.
D	Low risks , confirm that there are no low/no cost solutions which may eliminate/ reduce the risk further.
E	Trivial risk , no further action required but review at regular intervals to ensure controls remain effective.