jigsaw school
INSPIRED BY AUTISM

ONLINE SAFETY POLICY

Prepared By:	Jackie Charnock	Date Adopted:	July 2012
Job Title:	Assistant Director of Education	Status:	Non-contractual
Authorised By:	Emma Hawkins	Last Reviewed:	November2021
Job Title:	Director of Education	Ratified:	November 2021
Reviewed by:	Leetice Taylor	Next Review date:	November 2022
Job Title:	Deputy Designated Safeguarding Lead and Acting Educational Visits and Operations Coordinator	Version:	2.2

TABLE OF CONTENTS

1. Purpose

1.1 This policy sets out Jigsaw CABAS® School's procedures for Online Safety, building on best practice and government guidance. It covers all use of technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site.

1.2 This policy aims:

- To be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours.
- To ensure that pupils access the World Wide Web (internet) in a supportive and safe environment without fear of being bullied.
- To ensure staff are aware of their responsibilities regarding acceptable and safe internet usage procedures.
- To ensure measures are in place to make sure the security of ICT systems and devices is efficient and tested regularly.
- Online safety is a whole-school issue and responsibility, and pupils are supervised when accessing ICT equipment.

1.3 The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education, and business. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently into their chosen paths as adults.

1.4 Some of the benefits of using ICT and the internet in schools are listed.

1.4.1 For pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.

- Access to case studies, videos, and interactive media to enhance understanding.
- Individualised access to learning.

1.4.2 For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to other staff members and parents.
- Class management, attendance records, schedules, and reporting.

1.4.3 For parents:

- To have access to communication tools such as emails, Class Dojo, text messages and emails via Clarion Call, the School website, and the National Online Safety platform.
- The school staff can communicate daily in relation to their child's day, as well as receive updates and information through other communication devices.
- Parents can return communication in the same way.

2. Definitions

2.1 "Jigsaw" means Jigsaw School, Jigsaw Plus, Jigsaw Trust and Jigsaw Trading 2013 Limited (Café on the Park)

2.2 The "internet" is this policy is used to mean the route to the "World Wide Web" /" WWW" / "the web" as well as the pages found on the web as this is common terminology. We recognise that the internet is the route to accessing the web, not the pages, but in this context, it may mean both.

2.3 The "Director of Education" is the Head Teacher of the school.

2.4 Online safety is used to cover the internet, but it also covers mobile phones and other electronic communications technologies.

3. Scope

3.1 The Online Safety policy is an integral part of safeguarding children and relates to other policies including Safeguarding and Child Protection, Anti-Bullying, ICT Acceptable Use, Mobile Devices, Data Protection, Computing, Laptop, Bring Your Own Device (BYOD) and ICT Security Policies.

3.2 The policy also relates to statutory and non-statutory guidance such as Keeping Children Safe in Education 2021, The National Curriculum and Teaching online safety in schools.

3.3 The policy applies to all members of the Jigsaw School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

4. Implementation and Procedures

4.1 Online Safety Team

4.1.1 The Director of Education will appoint a senior member of staff to act as the Online Safety Co- ordinator.

Jayne Lobley Designated Safeguarding Lead

4.1.2 The Director of Education will also appoint another who in the absence of the Online Safety Co- ordinator will act as reserve Online Safety Co-ordinator

Carla Vaughan

Supervisor

4.1.3 Governor with responsibility for Online Safety

Adam Dalton

4.1.4 The above-named form the Online Safety committee along with Jigsaw Trust's

IT Technical Lead

4.2 Roles and Responsibilities

4.2.1 All members of staff have a responsibility to be aware of and adhere to all related ICT Policies.

4.2.2 The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

4.3 The Role of Governors

4.3.1 Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

4.3.2 A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include regular meetings with the Online Safety Co-ordinator and attendance at Online Safety Group meetings in which online safety incident logs will be evaluated, and reported as relevant at Governors meetings

4.3.2 Governors should take part in online safety training/awareness sessions at least annually.

4.4 The Role of The Director of Education

4.4.1 The Director of Education has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Team.

4.4.2 The Director of Education and (at least) another member of the School Management Team (SMT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

4.4.3 Members of the SMT are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

4.4.4 The SMT will receive regular monitoring reports from the Online Safety Team.

4.5 The Role of the Online Safety Co-ordinator and Deputies

- To promote an online safety culture under the direction of the management team.
- To maintain the school's Online Safety Policy, reviewing at least annually.
- To ensure that the Online Safety Policy links with other appropriate school policies e.g., Anti-Bullying, Safeguarding and Child Protection, Computing, Data Protection, and ICT Security Policy.
- To ensure the Online Safety Policy and its associated practices are adhered to.
- To ensure the IT Acceptable Use Policy/School internet rules are in place and up to date.
- To lead the Online Safety team and meet termly to discuss and evaluate current issues, review incident logs and filtering.
- To ensure staff receive regular training and relevant information about emerging issues and are aware of the procedures to be followed in the event of an online safety incident taking place.
- A planned programme of formal online safety training will be regularly updated and an audit of the online safety training needs of all staff will be carried out regularly.
- To ensure Online Safety is embedded in the curriculum, for example via assemblies and/or theme days (Safer Internet Day/Week, Anti-Bullying Week, etc.).
- To support Online Safety awareness initiatives for parents.
- To act as a point of contact, support and advice on Online Safety issues for staff, pupils and parents.
- To maintain an Online Safety Incident log to inform future online safety developments.
- To monitor, report and address incidences of pupils and staff accessing unsuitable online sites at school as necessary.
- To work in partnership with the IT Technical Lead to ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- To complete Online Safety audits annually, liaise with the nominated member of the governing body, and report to Board of Governors and School Management Team.
- To ensure Visitors who use IT equipment to present to the staff team or pupils for training sessions are asked to bring their own IT equipment or email their presentation before- hand. Guest devices must not be left unattended, and visitors are not left to present to pupils un-hosted.
- An annual online risk assessment to be carried out.

4.6 The Role of the IT Technical Lead

- To ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.

- To ensure that the school meets required online safety technical requirements and any relevant guidance that may apply.
- To ensure that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- To ensure children are safe from terrorist and extremist material when accessing the internet, through internet filtering/monitoring.
- To ensure servers, wireless systems and cabling are securely located and physical access restricted.
- To ensure all users have clearly defined access rights to school technical systems and devices.
- To ensure the Antivirus software is implemented.

4.7 The role of parents/carers

- To support staff in addressing concerns relating to their child regarding online safety.
- To sign a Responsible Internet Usage Consent Form on behalf of their child, and where appropriate discuss this with their child. (Appendices 1 & 2)
- To engage with digital communications sent by staff via the official school systems.

4.8 The Role of the Teaching and Support Staff

4.8.1 All other school staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, and understood the IT Acceptable Use Policy.
- They report any suspected misuse or problem to the Online Safety Team for investigation and action, either face to face, or through the online recording system CPOMS.
- All digital communications with pupils / parents / carers must be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- To ensure all pupils understand and follow the Online Safety Policy and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies regarding these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They attend and complete relevant online safety training.

5. Technical and organizational measures

5.1 Assessing Risks

5.1.1. Jigsaw CABAS® School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or the consequences of internet access.

5.1.2 Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

5.1.3 An annual risk assessment will be conducted to assess the risks in the online world at present and strategies put in place to reduce the risks.

5.2 Risk assessment, measurement and response

5.2.1 The School deem the risk of pupils misusing provided technology to be low.

5.2.2 There is a high teacher to pupil ratio and there are rarely occasions when a pupil is able to access a computer without a teacher present.

5.2.3 There is a managed filtering and monitoring system actioned by our IT Technical Lead and supervised by SMT.

5.2.4 Specific requested sites are blocked from access by pupils.

5.2.5 Pupils access the computer system via a password allowing limited access rights which do not permit access to blocked sites and staff user accounts.

5.2.6 Staff access the computer system and intranet via an individual log in with their own password, and access to Jigsaw user accounts are all individualised.

5.2.7 When not in use, all users will log out of their account on a device.

5.2.8 Data classification for drives and access rights are set out and updated when required.

5.2.9 Pupils do not use internet linked mobile phones at school.

5.2.10 Staff do not leave mobile phones in the classrooms without prior permission from senior management.

5.2.11 Staff using smartphones with school email accounts are required to keep them password protected, and on a timer to go into hibernate where the password needs to be input again to gain access to phone.

5.2.12 Personal devices with access to school email accounts will be required to use a multi-factor authenticator before accessing emails.

5.2.13 Staff using Jigsaw CABAS® School laptops out of hours are required to shut down the computer when not in use.

6. Monitoring

6.1 The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited)/filtering.

- Internal monitoring data for network activity.
- Surveys/questionnaires/discussions with pupils, parents/carers and staff.

7. Teaching Pupils about Online Safety

7.1 Many pupils also use ICT as a communication tool. It is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents/carers use it appropriately and practice good Online Safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online, and that it is everyone's responsibility to ensure the internet is used appropriately.

7.2 We know that some adults and young people use technology to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

7.3 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

7.4 A planned online safety curriculum will be provided as part of Computing / PSHE / other lessons and should be regularly revisited in line with DfE guidance "Teaching Online Safety in School" (June 2019)

7.5 Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key online safety messages will be reinforced as part of a planned programme of assemblies and themed events such as Safer Internet Day/Week.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to age-appropriate internet sites and monitored while using them.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be supported to have capacity to reduce the risks to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will be directed to age-appropriate internet sites and monitored while using them.

- Pupils must not use social media sites or chat rooms while in school. Some pupils have a school email account for internal emails only. Pupils with email accounts will be taught to tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account.
- Pupils will be taught to be careful not to reveal any personal information over email, or through the use of IT equipment.
- Pupils will be advised to never give out personal details of any kind that may identify them or their location.
- Pupils will be advised to never give out passwords.
- Online safety rules will be displayed in all classes.

8. Handling Online Safety Complaints and Concerns

8.1 A member of the School Management Team will deal with complaints of internet misuse, in the first instance the Online Safety Co-ordinator or Deputy will be contacted.

8.2 A CPOMS report will be written up, and once appropriate action has been taken, the report will be evaluated, and information fed back to school staff.

8.3 Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies.

8.4 Any complaint about staff misuse will be referred to the Director of Education.

8.5 Cyber-bullying by pupils whether in school, or incidents that take place outside of school, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Anti-Bullying Policy.**

9. Legislative Requirements

9.1 It is important to note that in general terms an action that is illegal if committed offline, is also illegal if committed online. It is recommended that legal advice is sought if any online safety concerns relate to illegal practice. Please see related legislation and guidance (12).

9.2 Guidance for Online Safety is sought from Keeping Children Safe in Education 2021, Independent Schools Standards 2014 and the Education Act 1996.

10. Policy Review

10.1 The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

10.2 This policy was last reviewed in November 2021.

11. Version History

No.	Date	Amendment
1.2	October 2019	7.6 Changes/deletions of role of the IT Support Engineer after consultation with the IT Support Engineer.
1.2	October 2019	8.2 Addition of DfE guidance "Teaching Online Safety in School" (June 2019)
1.2	October 2019	All reference to Internet amended to WWW (correct terminology)
1.3	June 2020	Appendix 1 and Appendix 2 added: forms for parents and pupils to sign
1.4	November 2020	1.2 before the bullet points "This policy aims:" inserted 2.2 "internet" defined in context of the policy to include the web /www / etc 4.4 do we need to refer to the fact that cyber-bullying is treat as serious whether it is in or out of school time? Added "whether in school, or incidents that take place outside of school" 6.5 Complete Online Safety audits annually added 6.5 "bring their own IT equipment" Added Visitors who use IT equipment to present to the staff team or pupils for training sessions are asked to bring their own IT equipment or email their presentation before- hand. Guest devices must not be left unattended and visitors are not left to present to pupils un-hosted. 7.2 "building resilience to radicalisation" Changed to "Pupils should be supported to have capacity to reduce the risks to radicalisation by providing a safe environment…." 15. Related internal documentation. All relevant policies added in this section and in policy if changes made Appendix 1 & 2 are acceptable use agreements. Section 3.13 states "Parents sign a Responsible Internet Usage Consent Form on behalf of their son/daughter, and where appropriate discuss this with their child." I have added (Appendices 1 & 2).
2.1	November 2021	Major policy rework.
2.2	June 2022	4.1 updated with change to Online Safety Coordinator and Deputy

12. Related Legislation & Guidance

Document	Location
Safer Internet Centre	https://www.saferinternet.org.uk/
South West Grid for Learning	https://swgfl.org.uk/products-services/onlinOnline Safety/
Childnet	http://www.childnet-int.org/
Professionals Online Safety Helpline -	http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation	https://www.iwf.org.uk/
CEOP	http://ceop.police.uk/
ThinkUKnow	https://www.thinkuknow.co.uk/
Computer Misuse Act 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents
Communications Act 2003	https://www.legislation.gov.uk/ukpga/2003/21/contents
Malicious Communications Act 1988	https://www.legislation.gov.uk/ukpga/1988/27/contents

Regulation of Investigatory Powers Act 2000	https://www.legislation.gov.uk/ukpga/2000/23/contents
Trade Marks Act 1994	https://www.legislation.gov.uk/ukpga/1994/26/contents
Copyright, Designs and Patents Act 1988	https://www.legislation.gov.uk/ukpga/1988/48/contents
Telecommunications Act 1984	https://www.legislation.gov.uk/ukpga/1984/12/contents
Criminal Justice and Public Order Act 1994	https://www.legislation.gov.uk/ukpga/1994/33/contents
Racial and Religious Hatred Act 2006	https://www.legislation.gov.uk/ukpga/2006/1/contents
Protection from Harassment Act 1997	https://www.legislation.gov.uk/ukpga/1997/40/contents
Protection of Children Act 1978	https://www.legislation.gov.uk/ukpga/1978/37
Sexual Offences Act 2003	https://www.legislation.gov.uk/ukpga/2003/42/contents
Public Order Act 1986	https://www.legislation.gov.uk/ukpga/1986/64/contents
Obscene Publications Act 1959 and 1964	https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66 https://www.legislation.gov.uk/ukpga/1964/74
Human Rights Act 1998	https://www.legislation.gov.uk/ukpga/1998/42/contents
The Education and Inspections Act 2006/2011	https://www.legislation.gov.uk/ukpga/2006/40/contents
The Protection of Freedoms Act 2012	https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
Serious Crime Act 2015	https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted
The School Information Regulations 2012	https://www.legislation.gov.uk/uksi/2012/1124/made

13. Related Internal Documentation

Document	Electronic Copy Location
Anti-Bullying Policy	Common / MyJigsaw / POLICIES / School /
Acceptable Use Agreement	Operations/PAWS/Parent Pack
Safeguarding and Child Protection Policy	Common / MyJigsaw / POLICIES / School /
Computing Policy	Common / MyJigsaw / POLICIES / School /
Data Protection Policy	Common / MyJigsaw / POLICIES / Trust /
ICT Acceptable Use Policy	Common / MyJigsaw / POLICIES / Trust /
ICT Security Policy	Common / MyJigsaw / POLICIES / Trust /
Mobile Devices	Common / MyJigsaw / POLICIES / Trust /
BYOD Policy	Common / MyJigsaw / POLICIES / Trust

APPENDIX 1 - Parent/Carer Acceptable Use Agreement

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to the World Wide Web (internet) at all times.

As part of your child's curriculum and the development of ICT skills, the Jigsaw CABAS ® School provides supervised access to the internet.

The Online-Safety Policy's aim is:

- To be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours.
- To ensure that pupils access the internet in a supportive and safe environment without fear of being bullied.
- To ensure staff are aware of their responsibilities regarding acceptable and safe procedures when accessing the internet.
- To ensure measures are in place to make sure the security of ICT systems and devices is efficient and tested regularly.
- Online safety is a whole-school issue and responsibility, and pupils are supervised when accessing ICT equipment.

Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. **If appropriate,** parents/carers are also requested to help their child complete the Pupil Acceptable Usage Form on the reverse of this form.

I understand that safeguarding is everyone's responsibility, including school, parents/carers, and we all have a duty of care to take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I will encourage my child ....to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed .... Date ....

PRINT NAME: ……………………………………………………………Relationship to Child: …………………………………………

APPENDIX 2 – Pupil Acceptable Use agreement

Pupil Acceptable Use

This is how we stay safe when we use computers:

- I will ask a teacher if I want to use the computers / tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of the computer and other I.T. equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): ....

PRINT NAME: ________________________________