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:	December 2022
Job Title:	Director of Education	Ratified:	January 2023
Reviewed by:	Jayne Lobley	Next Review date:	November 2023
Job Title:	Designated Safeguarding Lead	Version:	3.1

TABLE OF CONTENTS

1. Purpose

1.1 Technology is advancing rapidly and is now a huge part of everyday life, education, and business. We want to equip our pupils with all the necessary skills that they will need to enable them to progress confidently into their chosen paths as adults. 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

1.2 This policy sets out Jigsaw CABAS® School's procedures for Online Safety, building on best practice and government guidance. Online Safety is an integral part of safeguarding children and young adults.

1.3 The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable staff to work safely and responsibly to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns

1.4 Issues or concerns under online safety are categorized in 4 areas (the 4 Cs), including:

- Content – being exposed to illegal, inappropriate, or harmful material e.g. pornography, radical or extremist views.
- Contact - being subjected to harmful online interaction with other users, e.g. children can be contacted by online groomers
- Commercial exploitation – children can access platforms with hidden costs and advertising in apps, games, and websites
- Conduct – personal online behavior that increases the likelihood of, or causes, harm, e.g. making, sending, and receiving explicit images, online bullying …etc.

2. Definitions

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

2.2 'Jigsaw School', 'school' means Jigsaw CABAS® School

2.2 The 'internet' in 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 'ICT facilities' means all IT devices, facilities, systems, and services including, but not limited to, network infrastructure, intranet, internet, desktop computers, laptops, iPads and tablets, phones, personal organisers, music players, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.

3. Legislative Requirements

3.1 Jigsaw School acknowledges the statutory guidance of Keeping Children Safe in Education 2022 and non-statutory guidance of teaching online safety in schools.

3.2 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 (in section 12).

4. 4. Scope

4.1 This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet, and the use of technology, using devices provided by the school or personal devices.

4.2 The policy considers the requirements of statutory and non-statutory guidance such as Keeping Children Safe in Education 2022, The National Curriculum and Teaching online safety in schools.

4.3 The Online Safety Policy relates to other policies including:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- ICT Acceptable Use Policy
- Mobile Devices Policy
- Data Protection Policy
- Computing Policy
- Laptop Policy
- Bring Your Own Device (BYOD) Policy
- ICT Security Policy

5. Roles and Responsibilities

5.1 Jayne Lobley is the DSL (Designated Safeguarding Lead) responsible for online safety. The DSL is supported by the school's Online Safety Team, which includes 2 online safety coordinators, the school's IT manager and a school governor.

5.2 The online safety team is made up of the following staff & governor:

Jayne Lobley, DSL

Ros Clift, Senior Therapist & Online Safety Coordinator

Amber Jones, Senior Therapy Assistant & Online Safety Coordinator

Jake Spires, IT Manager

Owain Lewis, School Governor

5.3 All members of the school's community have important roles and responsibilities to play with regards to online safety.

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

The Role of Governors

5.5 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.

5.6 Governors should ensure that where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, and victims of abuse. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

5.7 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.

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

The Role of The Director of Education

5.9 The Director of Education has overall responsibility for online safety provision

5.10 The Director of Education ensures that online safety is viewed as a safeguarding issue and that practice aligns with Jigsaw's and national recommendations and requirements

5.11 The Director of Education ensures the school follows Jigsaw policies and practices regarding online safety (including Acceptable Use Agreements), information security and data protection

5.12 The Director of Education ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety

5.13 The Director of Education ensures that the DSL and Online Safety Coordinators have sufficient training, time, support and resources to fulfil their responsibilities

5.14 The Director of Education ensures that all staff receive regular, up to date and appropriate online safety training

5.15 The Director of Education and (at least) another member of the School Management Team (SMT) are aware of the procedures to be followed in the event of a serious online safety incident, and that there are robust reporting channels for online safety concerns

5.16 The Director of Education will receive regular monitoring reports from the Online Safety Team

5.17 The Director of Education ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

The Role of the Designated Safeguarding Lead

5.18 This is to:

- To take day to day responsibility for online safety
- To promote an awareness of and commitment to online safety throughout the school community
- To act as the named point of contact on all online safety issues, and liaise with other members of staff, or other agencies, as appropriate
- To keep the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- To facilitate training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- To monitor pupils' internet usage, and take action where required
- To maintain and review online safety logs and record of actions taken
- To report to the Director of Education, School Management Team and the Governing Body on incidents, internet filtering and monitoring, current issues and developments in legislation.
- To maintain the school's Online Safety Policy, reviewing at least annually.
- To lead the Online Safety team and meet termly to discuss and evaluate current issues, review incident logs and filtering.
- To ensure new staff receive online safety training as part of their safeguarding induction training.
- 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 work in partnership with the IT Manager 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.

The Role of the Online Safety Coordinators

5.19 This is to:

- Support and coordinate with the school's Designated Safeguarding Lead (DSL) and Safeguarding Team regarding issues relating to online safety
- Support the teaching team to understand when, and how to report online safety incidents and follow up on how they have been resolved where this is appropriate
- Meet with DSL, IT Manager and Governor responsible for Online Safety regularly to discuss incidents and developments
- Coordinate themed weeks and events related to online safety in the school, preparing and delivering activities for the pupils.

The Role of the IT Manager

5.20 This is to:

- To ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack while allowing opportunities to maximise learning
- 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.
- To maintain an up-to-date ICT Asset Register

The Role of the Teaching and Support Staff

5.21 All other school staff are responsible for ensuring that:

- They read, adhere to, and help promote the online safety policy, Acceptable Use Agreements and other relevant school policies and guidance
- Take responsibility for the security of school systems and the data they use or have access to
- They model safe, responsible, and professional behaviours in their own use of technology
- They embed online safety in their teaching and other school activities
- They supervise, guide, and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant
- They have an up-to-date awareness of a range of online safety issues and matters and how they may be experienced by the pupils in their care
- They identify online safety concerns and take appropriate action by reporting to the DSL for investigation and action, either face to face, or through the online recording system CPOMS.
- They know when and how to escalate online safety issues
- They take responsibility for professional development in online safety

- All digital communications with pupils / parents / carers must be on a professional level and only carried out using official school systems.
- 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. Staff should refer to the Mobile Device Policy for further information.
- 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.
- They are aware of appropriate conduct when taking part in virtual meetings.

The role of pupils

5.22 Where appropriate, pupils sign the Acceptable Use Agreement (Appendix 3)

- Follow online safety rules displayed in classrooms
- Use their own designated log in details to log in to devices and log out when finished.

The role of parents/carers

5.23 This is to:

- To support staff in addressing concerns relating to their child regarding online safety.
- To endeavour to keep their children safe online at home, following guidance from school where necessary
- To sign a Parent/Carer Acceptable Use Agreement on behalf of their child, and where appropriate discuss this with their child. (Appendices 2 & 3)
- To engage with digital communications sent by staff via the official school systems.

The role of visitors

5.24 Visitors who use ICT equipment to present to the staff team or pupils for training sessions are asked to bring their own ICT 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.

6. Reducing Online Risks

6.1 The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The Jigsaw CABAS® School will take all reasonable precautions to prevent access to inappropriate material.

6.2 An annual risk assessment will be conducted using the 360 safe website to assess the risks in the online world at present and put strategies in place to reduce the risks.

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

6.4 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.

6.5 There is a managed filtering and monitoring system actioned by our IT Manager and supervised by SMT. This meets the Keeping Children Safe in Education 2022 guidance of 'appropriate levels' without 'over blocking' and limiting pupil's exposure to risks in order to learn the importance of keeping safe online.

6.6 Specific requested sites are blocked from access by pupils.

7. Safer Use of Technology

7. 1 Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

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

7.3 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.

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

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

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

7.7 Staff do not use mobile phones in the classrooms without prior permission from senior management.

7.8 Visitors to the school do not bring mobile devices into pupil areas without prior permission from the SMT.

7.9 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.

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

7.11 In the event of devices being lost or stolen, the IT Manager will wipe content from the device remotely

7.12 Staff using the school's laptops out of hours are required to shut down the computer when not in use.

8. Education and Engagement

8.1 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.

8.2 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.

8.3 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.

8.4 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)

8.5 Online Safety can be categorised into four areas of risk, content, contact, conduct and commerce, as stated in Keeping Children Safe in Education 2022, and these four categories will provide the basis of 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 will be taught to be careful not to reveal any personal information over email, or through the use of ICT 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.

9. Training and Engagement with Staff

9.1 The School will:

- Provide and discuss the Online Safety Policy and Staff Acceptable Use Agreement with all staff as part of their induction
- Provide up-to-date and appropriate online safety training on a regular basis, with at least annual updates
- Make staff aware that school systems are monitored, and activity can be traced back to individual users
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within the school
- Highlight useful educational resources and tools which staff could use, according to the age and ability of pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

10. Awareness and Engagement with Parents and Carers

10.1 Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

10.2 The School will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats, for example, newsletters, school website information and links to useful resources and tools
- Informing parents about what the School asks pupils to do online, and who they will be interacting with
- Drawing parents' attention to the School's Online Safety Policy and expectations
- Requiring parents to read and sign the parent/carer and pupil *Acceptable Use Agreement (please refer to Appendices 2 and 3)* and discuss its implications with their children

11. Responding to Online Safety Incidents, Concerns and Complaints

11.1 All members of the school community must respect confidentiality and the need to follow the official school procedures for reporting concerns. Procedures for reporting will be dependent on the category of the four areas of risk, as stated in Keeping Children Safe in Education 2022. Please see Appendix 1

11.2 After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required

11.3 If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the relevant agencies

11.4 If an incident or concern needs to be passed beyond the school community (i.e. other schools being involved or the public may be at risk), the school will contact the Police or Local Authority first, to ensure that potential investigations are not compromised.

11.5 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.

11.6 The DSL will inform parents/carers of any incidents or concerns involving their child, as and when required

11.7 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.

12. Managing Personal Data Online

12.1 Personal data will be collected, processed, stored and transferred and made available online in accordance with the Data Protection Act, 2018 and General Data Protection Regulations, 2018. Please refer to the School's Data Protection Policy and privacy notices on the school's website.

13. Social Media

13.1 The term social media includes (but not limited to): blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video and photo sharing sites, chatrooms and instant messenger

13.2 All members of the school community are expected to engage in social media in a positive, safe and responsible manner at all times

13.3 The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff at induction and is revisited and communicated via regular staff training opportunities of staff meetings

13.4 The use of personal social media sites are not permitted for staff outside of their allocated break times during school hours

13.5 Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct, staff Acceptable Use Agreement policies

13.6 Safe and appropriate use of social media will be taught to pupils as part of online safety education using age appropriate resources and considering pupils' abilities

13.7 The school will not create any personal social media sites for any pupils

13.8 The use of personal social media during school hours is not permitted for pupils

14. Monitoring and Review

14.1 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.

14.1 The Online Safety Policy will be reviewed annually by the Designated Safeguarding Lead, 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.

14.2 This policy was last reviewed in November 2022.

15. 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
2.3	November 2022	Updates to Deputy Online Safety Coordinator and Governor responsible for Online Safety. Update job title of IT Manager. Insertion at 5.2.11 that 'Visitors to the school do not bring mobile devices into pupil areas without prior permission from the SMT.'
3.1	December 2023	Policy rework following governor feedback on the policy. Addition of appendix 1 to show categories of concern and how to report and respond to them.

16. 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
UK Council for Internet Safety (UKCIS)	UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young adults

17. 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 Device	Common / MyJigsaw / POLICIES / Trust /
BYOD Policy	Common / MyJigsaw / POLICIES / Trust

APPENDIX 1 – Categories of Concern

<table>
<tr><th rowspan="2">Category of concern</th><th colspan="2">How to report</th></tr>
<tr><th>Pupils</th><th>Staff</th></tr>
<tr><td>Content - being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism</td><td rowspan="3">Pupils will be taught to tell a member of staff if they are exposed to inappropriate or unsuitable content when online.

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 are encouraged to tell a member of staff if they have been harmed or threatened to be harmed, when online. This includes any type of abuse, but in particular cyberbullying, emotional abuse, grooming, sexual exploitation and sharing of explicit images. Pupils are taught not to view other children's images if they are aware of them.</td><td rowspan="2">Smoothwall filtering system automatically notifies the DSL and Deputy DSL when access to "inappropriate" content has been blocked. Staff must immediately advise a member of the safeguarding team if they observe a concern related to content, contact, or conduct and follow up by writing a CPOMS report for an online safety concern.

The DSL or Deputy DSL will ensure that online safety concerns are escalated to and reported to relevant agencies where necessary, including referrals to the Police if there is a suspicion that illegal activity has taken place, or Prevent if there is a concern related to extremism or radicalisation.

Staff must not intentionally view any nudes or semi-nudes unless there is good and clear reason to as stated in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young adults</td></tr>
<tr><td>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.</td></tr>
<tr><td>Conduct: 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,</td></tr>
<tr><td>Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.</td><td></td><td>Staff must report immediately to the DSL or Deputy DSL if they have a concern relating to Commerce. The DSL/Deputy will report to the IT Team to confirm the authenticity of the email or website and access will be blocked where necessary.</td></tr>
<tr><td colspan="3">All online safety concerns should be reported immediately to the Safeguarding Team – staff must not ignore their suspicions and should not assume that someone else will take action to protect an individual.</td></tr>
</table>

APPENDIX 2 - 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 3 – 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: _____