we are an i-vengers school

CHANGING CHILDREN'S WORLDS • INSPIRING • EXPLORING • LEARNING
Brackenfield SEND School

East Midlands
SEND Training Hub

Online Safety Policy

Policy Owner	Sophie Evitts
Role	Deputy Headteacher
Date issued	June 2022

Controlled upon completion

DESIGNATED SAFEGUARDING LEAD (S): MICK GAYLE

NAMED GOVERNOR WITH LEAD RESPONSIBILITY: KIM HAMBLETT

CONTENTS

Page no

POLICY AIMS

- This online safety policy has been written by Brackenfield SEND School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input, and reformatted and with additions, with permission by the Child Protection Manager for schools/education, Derbyshire county council as required.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' , Early Years and Foundation Stage (insert only if applicable) 'Working Together to Safeguard Children' and the Derby and Derbyshire Safeguarding Childrens Partnership Safeguarding procedures.

- The purpose of this online safety policy is to:
  - Safeguard and protect all members of Brackenfield SEND School community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role 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.

- This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

POLICY SCOPE

- Brackenfield SEND School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Brackenfield SEND School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Brackenfield SEND School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 LINKS WITH OTHER POLICIES AND PRACTICES

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use policy
- Code of conduct/staff behaviour policy
- Behaviour policy
- Child protection policy
- Confidentiality policy
- Teaching and Learning Policy
- Data security

MONITORING AND REVIEW

Technology in this area evolves and changes rapidly. This school will review this policy at least annually.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the H*ead teacher/manager* will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

ROLES AND RESPONSIBILITIES

- The Designated Safeguarding Lead (DSL) Mick Gayle, has lead responsibility for online safety. ***Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.
- Brackenfield SEND School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 THE LEADERSHIP AND MANAGEMENT TEAM WILL:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and/or* acceptable use policy, which covers acceptable use of technology. (***Amend as appropriate***)
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.

- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

THE ROLE OF THE DESIGNATED SAFEGUARDING LEAD

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly every 10 weeks as part of the MER cycle, with the governor with a lead responsibility for safeguarding and online safety.

STAFF RESPONSIBILTY

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime, and make a Cyber Choices referral.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. The school used the standard LA Internet Service Provider, which is **Broadband and web-filtering is provided by RM PLC**.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement *and/or* acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.

- Use our systems, such as learning platforms, and other network resources, safely and appropriately; Teams and Office 365 apps monitors by the IT Manager, Busy Things monitored by class teachers
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

EDUCATION AND ENGAGEMENT APPROACHES

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
    - The school follows the iVengers Special Agents Scheme of Work (see appendix for content)
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology. (Headteacher Awards)
- Implementing appropriate peer education approaches. (Special Agents)
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- ○ Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 VULNERABLE LEARNERS

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modeling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home. There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

- Brackenfield SEND School recognises all learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Brackenfield SEND School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum Brackenfield SEND School will seek input from specialist staff as appropriate, including the Online Safety Lead (Sophie Evitts) and Child in Care Designated Teacher (Sophie Evitts).

5.3 TRAINING AND ENGAGEMENT WITH STAFF

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis, with at least annual updates.

    - The Online Safety Lead delivers annual online safety training, written alongside Online Safety Advisor, Traci Good
    - Staff also complete online trianing via EduCare to reinforce their learning
    - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 AWARENESS AND ENGAGEMENT WITH PARENTS AND CARERS

- Brackenfield SEND School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We 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.
        - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

REDUCING ONLINE RISKS

- Brackenfield SEND SChool recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.
-

SAFER USE OF TECHNOLOGY

7.1 Classroom Use

- Brackenfield SEND School uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community; SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.

- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age, ability and developmental milestones.

    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - **Key Stage 2**
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.
    - **Key Stage 3, 4, 5**
        - Learners will be appropriately supervised when using technology, according to their ability and understanding. (***Amend as appropriate***)
    - **Learners in residential provision**
        - We will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe
          Practice by children in accordance with the national minimum standards (NMS).

7.2 MANAGING INTERNET ACCESS

- We will maintain a written record of users who are granted access to our devices and systems.

- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

- We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly

7.3 FILTERING AND MONITORING

The school used the standard LA Internet Service Provider, which is Broadband and web-filtering is provided by RM PLC.

Content filter

Our Internet Provider uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

Security and virus protection

The school uses Microsoft Windows Defender Antivirus software. The software is monitored and updated regularly automatically by Windows updates.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the IT Manager

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

7.3.1 DECISION MAKING

- Brackenfield SEND School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 FILTERING

- Education broadband connectivity is provided through RM PLC.
- We use RM PLC which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with RM PLC to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
  1. Making a note of the website and any other websites linked to it.
  2. Informing the IT Manager (checking the blocking rights already in place)
  3. Discussion with the pupil about the incident, and how to avoid similar experiences in future
  4. Explaining to all staff and pupils what type of sites will be blocked

  Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.

7.3.4 MONITORING

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services. If a concern is identified via monitoring approaches;
  - It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.
  - Due to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
  - Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded
    - Interview/counselling by class teacher, Senior Leadership Team (including a DSL and the Head Teacher)
    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - referral to LA / Police.
    - Our DSL's act as a first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher. Any safeguarding concerns are reported to the Designated Safeguarding Lead.
    - All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

- If a concern is identified via monitoring approaches we will:
    - Respond in line with the child protection policy
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 MANAGING PERSONAL DATA ONLINE

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our GDPR handbook (Teams-Polcies-GDPR)

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.

  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all but the youngest users. (Note: this should be in place for all except Early Years and Foundation Stage children and some learners with SEND)
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be found at:
    - Acceptable Use of IT Policy

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- If using online recording systems e.g. a CP record system restricted access will be granted per job role and responsibility with regular reviews of who has access
- When the pupil is developmentally able to recall a password independently, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system - the longer and more unusual, the stronger it becomes. Using a combination of upper, lower case, numbers and special characters is recommended.
  - Change their passwords every XXXXX
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

7.6 MANAGING THE SAFETY OF OUR WEBSITE

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 PUBLISHING IMAGES AND VIDEOS ONLINE

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 MANAGING EMAIL

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Mick Gayle, Head of Pastoral Care, if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

7.8.1 STAFF EMAIL

- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
- Members of staff will refer to and adhere to the acceptable use policy and any other policy where staff use of mobiles is referred to.

7.8.2 LEARNER EMAIL

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

7.9 EDUCATIONAL USE OF VIDEOCONFERENCING AND/OR WEBCAMS

Brackenfield SEND School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.

- All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 USERS

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.

- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learner's age and ability.
- Pupils will not access web cams or video conferencing unsupervised. Staff will ensure contact details shared are school details and not personal.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 CONTENT

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 MANAGEMENT OF LEARNING PLATFORMS

- Brackenfield SEND School uses BOOP as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.

- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 MANAGEMENT OF APPLICATIONS (APPS) USED TO RECORD CHILDREN'S PROGRESS

- We use BOOP to track learners progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.

  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8.1 SOCIAL MEDIA EXPECTATIONS

- The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of Brackenfield SEND School community.
- Members of staff will refer to and adhere to the schools social media policy and any other policy where the staff use of social media is referred to.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
- Concerns regarding the online conduct of any member of Brackenfield SEND School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 LEARNERS PERSONAL USE OF SOCIAL MEDIA

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
  - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:

    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

USE OF PERSONAL DEVICES AND MOBILE PHONES

- Brackenfield SEND School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

STAFF USE OF PERSONAL DEVICES AND MOBILE PHONES

- Members of staff will refer to and adhere to the schools acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to.

9.2 LEARNERS USE OF PERSONAL DEVICES AND MOBILE PHONES

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Brackenfield SEND School expects learners' personal devices and mobile phones to be on silent and secure, supervised by staff.
- If a learner needs to contact his/her parents or carers they will be allowed to use a classroom phone.
    - Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher

- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
    - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
    - Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy. ***See*** www.gov.uk/government/publications/searching-screening-and-confiscation)
    - Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. ***See*** www.gov.uk/government/publications/searching-screening-and-confiscation)
    - Mobile phones and devices that have been confiscated will be released to parents or carers or via transport providers at the end of the school day
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.3 VISITORS' USE OF PERSONAL DEVICES AND MOBILE PHONES

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

9.4 OFFICIALLY PROVIDED MOBILE PHONES AND DEVICES

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community will be made aware of the availability of the Cyber Choices early intervention programme for individuals who are involved in cybercrime, or those who are gifted and talented and are at risk of becoming involved in cybercrime.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- We will refer to the flow chart on responding to incidents, made available

- Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headteacherwill speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.

10. CONCERNS ABOUT LEARNERS WELFARE

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11. PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

11.1 ONLINE SEXUAL VIOLENCE AND SEXUAL HARASSMENT BETWEEN CHILDREN

- Our school/ setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.
- Brackenfield SEND School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

- Brackenfield SEND School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Brackenfield SEND School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Brackenfield SEND School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. The iVengers special agents scheme of work is an appendix to this policy.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.

- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 YOUTH PRODUCED SEXUAL IMAGERY (“SEXTING”)

- <*Setting name*> recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ and KSCB guidance: “Responding to youth produced sexual imagery”.
- Brackenfield SEND School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board’s procedures.
    - Ensure the DSL (or deputy) responds in line with the ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.

- Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION (INCLUDING CHILD CRIMINAL EXPLOITATION)

- Brackenfield SEND School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Brackenfield SEND School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community via our school website
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
  - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

11.4 INDECENT IMAGES OF CHILDREN (IIOC)

- Brackenfield SEND School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the Headteacher is informed in line with our managing allegations against staff policy immediately and without any delay.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

11.5 CYBERBULLYING

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Brackenfield SEND School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy. (**Teams-policies-safeguarding)**

11.6 ONLINE HATE

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Brackenfield SEND School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

11.7 ONLINE RADICALISATION AND EXTREMISM

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- All concerns will be reported to the DSL (or deputy DSL) and dealt with in accordance with the policy.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

11.8 CYBERCRIME

- Cybercrime incidents and offences will be responded to in line with our existing behaviour policies.
- We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.
- We will make a Cyber Choices referral for early intervention, as per the Cyber Choices toolkit.
- If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit

https://www.saferderbyshire.gov.uk/what-we-do/cyber-crime/reporting-cybercrime/digital-mot/digital-mot.aspx

USEFUL LINKS FOR EDUCATIONAL SETTINGS

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children Partnership on line procedures DDCSP:

- http://derbyshirescbs.proceduresonline.com/

Derbyshire Police:

- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Derbyshire Police via 101

LADO

- By referral into Professional.Allegations@derbyshire.gov.uk
- Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

- Immediate risk of harm phone 01629 533190
- For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
- For professional advice phone 10629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

APPENDIX -IVENGERS SPECIAL AGENTS

VISION AND ETHOS

Designed for pupils with SEND, Special Agents mission is to:

- Promote safe, positive online activity in a digital world
- Develop and maintain digital resilience
- Understand and recognise the risk of being online and demonstrate how to apply online safety rules

WHY SPECIAL AGENTS?

Pupils will SEND struggle to transfer skills learnt in the classroom to the outside world. Often pupils with SEND can verbalise a rule and recite how to stay safe but fail to notice the risks when they occur in the moment. Pupils with SEND are often captivated by devices and technology, with skills which surpass their generalised ability to access the world around them. This too causes additional risk and vulnerability as pupils are exposed to potential risks by chance. Pupils with SEND maybe developmentally and cognitively impaired, however more often than not, their online experience is similar to their neuro-typical peers. Special Agents creates an open dialogue with pupils, staff and parents about what pupils are doing online and how to do it safely.

Special Agents is focused on immersive learning creating a positive digital world common language embedded in the school community.

The main objectives are:

- To create a digital persona
- To demonstrate how digital life should be
- Facilitate positive online experiences
- To open up access to the positive digital world
- Facilitate in the moment problems leading to problem solving
- Learn the steps to access content we want
- To support peers with learning

CREATING A DIGITAL WORLD IMMERSIVE ENVIRONMENT

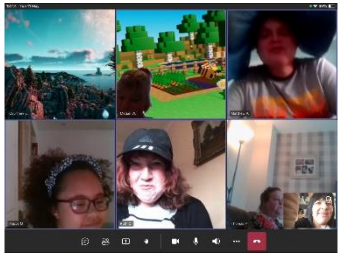
At Brackenfield, online safety replicates the curriculum models. We immerse pupils in online activity which is accessible to them supporting progress through motivators, strengths and needs. We promote positive online experiences to enrich pupils' opportunities in a digital world.

You Tube is the most common online experience in school. It starts at home; families use You Tube to motivate even the most complex SEN needs at home and support regulation.

Within the informal curriculum, pupils have videos embedded into routines. Videos are shared with home and chosen to reflect pupil interests. Our immersive classroom is interactive, along with our sensory rooms and portable sensory projector- promoting cause and effect opportunities. iPads are used to take photos to support communication in the moment- to improve clarity of messages, to support pupil understanding and decision making.

In the semi formal curriculum, pupils also use videos to listen to stories, learn new signing, make and watch videos of themselves and their friends as well as help structure their day. Pupils have access to iPads with games focused on early maths and literacy skills- as well as early communication. Pupils continue to use YouTube but for enjoyment purposes- this ever-growing sense of independence on an iPad has huge impact on confidence. Pupils explore desktop devices to draw, find photos of interest, play games and communicate with peers.

All pupils have Teams accounts. These are used for video calls with pupils who are at home, if they wish to engage with lessons in school. Classes call other classes within school too. Pupils can access Teams outside of school. This platform is promoted for pupils to message each other in the chat function. This is monitored by staff and when problem arise can be addressed straight away in the classroom. Pupils use Microsoft applications as part of the independent living curriculum, on laptops and iPads. This not only teaches them the skills to use these but opens up accessibility from home as well. Visually impaired pupils are taught the steps to use audio features and increase font size etc. Pupils are taught the importance of keeping passwords safe and changing them. This is a hard but necessary life lesson- knowing how to reset your password.



We host virtual enrichments- including both primary and secondary aged pupils. This happens after school via Teams. Pupils have a focus for the session, it might be games or an arts and crafts club. This is chosen through pupil voice. School supply arts materials for pupils to take home and complete the project over Teams. Staff are also involved as role models, to model expectations replicating what we do in school.

Pupils use devices to take their own photos to support recalling information, sequencing, comprehension and communication. Pupils are given problems to solve to teach online safety rules, in contexts they access, to ensure safety is transferable and not just a learned script which is not applied.

In the formal curriculum, pupils are equally as immersed as all the other pupils across school. In this curriculum model it is very clear how pupils can navigate and manipulate the digital world with low levels of literacy and numeracy. We are keen to empower our students to be confident in a digital world- where usually they would feel vulnerable and different. Pupils take part in virtual enrichment, daily communication between friendship groups on platforms set up by school. By introducing Teams, pupils have moved away from games like Roblox to communicate. This has reduced the risk online as Teams is secure and managed by school. By promoting positive online activity and celebrating it- emailing opportunities to staff and peers, blogger style videos, onsite games consoles, iPads and curriculum apps- pupils have learned online experience to transfer at home. We continue to remind of rules and risks applicable to the activities the pupils do.

SPECIAL AGENT MISSIONS

iVengers Special Agents should be delivered as an introduction to all pupils who show an interest in regular use of technology. Sessions should be consistent, structured and part of routine. Ideally once a every two weeks as a group, then revisited within the class group. Special agents should also have a newsletter slot with a 'did you know' fact. Tasks have a starter, main and plenary to promote consistency and support delivery/ focus.

Task	Purpose	Descriptor	Rationale	Resources
Special Agents Launch Assembly	To explain what Special Agents will do and provoke interest	10-15 mins Present the purpose of special agents in school, including: - Their role - -how often they will meet - Technology in school - Some examples of how they will help peers and staff - Some suggested names/ missions	To introduce pupils to Special Agents in a format accessible to them	Example PPT/ video Template PPT to be adapted by schools
Mission 1: **Apply to be a special agent**	To answer key questions about why promoting online safety is the right thing to do	Send secret mission video to classes, asking pupils to record a short video explaining why they want to be a special agent, what their name would be and their superpower online. Or present in photos or drawing format. Pupils film video and send to chief agent to be chosen for panel. Drawings/ photos are displayed in school to raise profile of special agents. Meet group of selected members, for an initial photo before launch meeting.	Recording videos and recalling purpose of Special Agents helps pupils articulate what they are doing and why. Using technology helps to embed the principles of using technology positively as well as using new skills. Taking a group photo gives pupils an outcome of their application and reassures anxieties.	Example secret mission video Template for photo montage Template for drawing Access to online gallery of other special agents

		Plenary:		
Mission 2: **Special Agents meeting**	To walk through what Special Agents will do; frequency of meetings, who will lead it and share ideas for mission 3	Meet pupils in groups. Maximum groups of 5 pupils work best. If you can assign a TA to each group, this will support workload and dissemination of the tasks. Use minute template to show meeting content. Try and add photos from school to support recall and understanding: -Where meetings happen -Who meetings are with -When meetings will happen -How long they will be -Format of meetings (show template of minutes) -Discuss some common rules for the group to be read at the beginning of each session -Ask for any questions -Explain mission 3 and discuss some basic ideas	Walking through how meeting swill run will support anxiety of pupils and support pupils eventually leading sessions themselves. Pupils will be able to recall what happens next, or what happened the week before and what will happen next week. Pupils will know what to expect when they come to meetings which means they will be more confident when taking part in sessions. Establishing simple rules will make expectations clear and make nervous pupils feel safe.	Meeting minute template Storyboard template for photos of meeting format Question box/ form or email address for pupils to access in between meetings if appropriate
Mission 3: **Design your digital persona**	To role model digital persona and showcase examples, highlight digital persona can be the best bits of you (Discussing privacy/ consent)	Review group rules Starter: Show some examples of digital persona and match to real life people; using staff emojis in school is the most impactful. Main: Go through digital persona for chief agent and then go around the group and discuss best bits of you for digital persona, asking	Using staff pupils know makes it easier for them to relate to, as the concept becomes less abstract. Ensuring you discuss consent means you begin to embed the notion of consent and it becomes a natural question student asks themselves when online 'do I want people knowing that about me?'	Example digital avatars/ emojis Storyboard template of mission for pupil recall

	Key question: What do you want people to think?	specifically what do you want people to think about you? Discuss some examples to be clear we are not lying about who we are, but only sharing what we want to. Plenary: Ask pupils to recall the task, discuss the format of the design. Give a deadline and assign TA to support group with the completion of this mission.	Recalling the task allows you to clarify understanding and also assign support where some pupils might be confused. Using a set of visual instructions will help promote independence for pupils to follow on their own or with limited support.	
Mission 4: **Create your digital persona**	Step by step creation of digital persona, working in a group to edit photos, use AR apps, film GIF-hiding true identity	Go over simple rules of group, led by pupil recall. Starter: Ask pupils to share their digital persona designs and give feedback between the group. Main: Working in 2s or 3s to design digital personas on app. Plenary: Share digital personas as a group. Chief agent will merge all digital personas and share school wide. Pupils will present the video to their classes, where appropriate.	This task promotes teamwork, using simple technology for positive outcomes, promotes using new apps and helping each other whilst continuing to represent the Special Agent team. Pupils will give each other feedback and prompts to use the apps and once they have made their personas. These personas will follow the pupils for the full year, showing how digital presence doesn't disappear and what you chose to share is seen by lots of people.	List of apps to use to make digital personas; GIFs, AR, photo editing apps, emoji apps

Mission 5: **Capture digital world experience of special agents**	To gauge starting point of group and key motivators online	Review simple group rules. Starter: Explain mission is to share experiences online. Give some examples of other children and what they do at different ages. Main: Go through set questions to gauge understanding of group and their exposure online. There are some key words to discuss for understanding and use in context. Plenary: Summarise what the group have shared, highlighting what is the same and any differences.	Finding the starting point of the group allows you to target key areas and stops generic online safety delivery, increasing impact of the group.	Meeting minute template Key question list Key terminology list
Mission 6: **Complete a staff survey**	To introduce Special Agents to wider school community, identify strengths of Special Agents vs. staff, to empower Special agents to support everyone in the community	Review simple group rules. Starter: Review group experiences last session and introduce staff survey to groups. Main: Assign special agents to ask staff across school. Assign a TA to support collection of data. Survey is on a form. Plenary: Recall with group who is asking who and what the timescale is.	This task is designed to empower pupils as it is highly likely they can do things on different types of technology staff are unable to do. It is also likely pupils know the latest trends which some staff will not have heard of.	Survey examples: Microsoft forms Google forms

		Pupils could film a video for staff to promote the survey if they wish.		
Mission 7: **Create a staff advice video**	Raise presence of Special Agents and begin articulating online advice, not just safety related- capturing skills and signposting. Staff can also feedback to Special Agents reaffirming their skills as Special agents.	Recall simple group rules. Starter: Review staff survey results, highlighting to pupils where staff are not confident, and they can offer advice. Main: Script the format of the video, with pupils taking key lines of advice each. Format script in the style of 'you said….' 'If you do this…….' 'Have you tried….' 'Did you know……' Film video on video making app, using a director from the group. Plenary: Review video with group and add additional features using the video making app. Email out to staff and pupils can share with staff in their classes. Groups should show the leadership team. Chief Agent will collect feedback from staff.	Pupils feel more confident in their abilities online and naturally recall safe practices to offer advice to staff. They do not feel threatened because they are the ones offering advice, which often leads to some disclosures about unsafe practices- which can be addressed as part of the group.	Example video List of video making apps:
Mission 8: **Complete a pupil and**	Write a series of questions based on staff feedback about pupil habits and	Review simple group rules. Starter:	Pupils will feel confident using current terminology because they have been meeting for a few weeks now. You will know what they know, and this will	Example survey questions to help frame questions

parent survey	their experience with parents to inform them of survey and direction of questions to pupils and parents	Review content of staff advice video and the feedback from staff. Discuss what the questions should be for pupils and their parents. Main: Write survey for with pupil and parent questions. Decide if you want to use the same survey or two different ones. If you have multiple groups, you can split parent and pupil survey between them, or do half a survey each. Plenary: Film short video to introduce the survey and asking people to complete it and send out to all parents and pupils. Ask class teams to complete in school time to support accurate reflection of online habits of pupils. You could set up a QR code for parents to complete and send out on paper as prompts.	influence what they ask. You will use some open-ended questions, so topics can come back which you might not have thought of, and this can be explored with the group. It is important to remember pupils cannot generalise abstract leanring, so the advice and guidance for the wider school must be related to their online habits and cannot be generic advice.	
Mission 9: **Discuss key results of survey**	Highlight difference between themselves and their peers, as well as difference between pupils and parents- discussing what parents are scared of online	Recall simple group rules. This should be pupil led now. Starter: Review staff survey and then pupil and parent survey format. Discuss results of survey. Main:	Pupils will be able to recall what their peers do online and how that is different or the same as them. You will be able to establish top apps and social media usage in school, helping you target advice and also focus staff trianing where appropriate.	Survey results

		Go through differences between parents and pupils. Discuss key themes for both groups and any similarities. Go through what parents are scared of and how we might help them feel less scared. Plenary: Recall findings as a group and walk through the next mission for a parent/ carer advice video, discussing ideas.		
Mission 10: **Create a parent/ carer advice video**	Use discussion notes to identify key pieces of advice for parents and carers, signposting to online advice and guidance	Recall simple rules. Starter: Recall notes from the parent results. Main: Script the format of the video, with pupils taking key lines of advice each. Format script in the style of 'you said….' 'If you do this…….' 'Have you tried….' 'Did you know……' Film video on video making app, using a director from the group. Plenary: Review video with group and add additional features using the video making app	Pupil are continuing to use key terminology and experience positive use of technology. Pupils are able to recall key advice again and also listen to why parents might not be worried about their children. It is key to remember pupils with SEND might not be ablet empathise, not see why parents worry, so this activity might need to be shared with staff members for pupils to see their reactions and give direct feedback about why it is good advice for parents.	Example video List of video making apps:
Mission 11:	To use photo editing applications to see how real-life photos	Pupil led recall of simple group rules. Starter:	Pupils might not be able to understand the concept of something being fake or not real. This is why it is important o work	Real and fake selfie examples

Healthy Selfies	can change to fake ones. Use language to show how things change.	Discuss different ways photos can be edited and do some live examples. Main: Create additional selfie edits, and judge in groups whether they are real or fake. Print off photos before and after edits for special agents to take back to class to discuss with peers. Remember to constantly recall the key terminology. Discuss when things being faked could upset others. Plenary: Ask pupils to recall when something is fake, and it can upset others. Ask pupils to recall game to take back to peers and also ensure all special agents can recall the 'fun' and how to look after themselves and friends.	through the tasks, changing faces etc using apps and showing how things can change. Children and adults with additional needs are extremely vulnerable to fraud and being taken advantage of because they do not understand concepts they have not experienced. Using the words fake and consent in context as often as possible will allow pupils to eventually understand the concepts and make their own choices. Discussing when people might be upset, develops social understanding and also allows pupils to recognise when something might upset them.	Photo editing apps:
Mission 12: **Create 'Go to' lists of key interest of school population and publish on website**	Pupils will list all the places they use online and also then see what other pupils use- have a go in school and then send out to all classes- presenting to their own class and publish on the website	Review class rules, led by pupils. Starter: Brainstorm the themes amongst pupils again, and list key areas of signposting for pupils. Main: Assign themes for groups to write lists for and find the website links for. Plenary: Review as a group and discuss themes and where any gaps are.	Pupils experience and promote positive online experiences led by pupil interest. This stops pupils straying into risky sites and will promote positive algorithms in their search histories on social media etc. Having a page on the website you can direct pupils to, reduces the number of clicks online, promotes using safe sites, gives purpose to being on the school website and support parent anxieties about safe websites to visit.	Website sharing template

		Chief agent can compile list in sharable format and update on school website and share with pupils/ parents.		
Mission 13: **Create video reviews of online activities**	Review popular online activities to promote them amongst community and also highlight top tips to make them even better!	Pupil led recall of rules. Starter: Recall popular games from pupil survey and discuss views; what it is about, what is good, what is bad, top tips. Main: Assign groups to film short reviews following the same questions as above. What it is about, what is good, what is bad, top tips. Ask pupils to take screenshots on devices of images linked to game to add to the video- this supports recognising game and also embeds skills on different devices. Plenary: Watch short videos, decide on format of the videos- one long review or short videos for each game. The chief agent will format the videos and upload to the website, then share with special agents and families.	Gaming is popular with all young people and comes with risks when using websites and apps with purchases in etc. Showcasing games which are safe and fun, will support pupils trying the right ones and forge good habits when gaming. This positive experience activity leads onto discussing the risks which need addressing, but we need to know what we should be doing first, to then understand why something might be a risk to us.	List of online gaming websites Example review videos
Mission 14:	Discuss online trends (videos/ games/ chats etc.) to	Pupils to recall rules. Starter:	This session might need repeating and also following up with a repeat in classrooms	Key terminology list

Quick reflexes	highlight risks and practise reacting to risks	Recall gaming reviews and popular websites. Discuss risks or dangerous things, or things parents worry about. Main: Map out quick fixes when a risk occurs; name risk, the problem and dangers and then a 'quick reflex'. Discuss superpowers and fighting off danger in disguise. Pupils might make disclosures here, so be vigilant. Where some obvious risk and dangers are not discussed, feed these in to ensure you cover risks i.e., talking to strangers, hidden costs, viruses etc. Plenary: Send agents away to discuss risks online in their class groups so they can bring some more to the group to help advice videos. TAs need to collate information from class groups, so advice videos are meaningful.	because risks are an abstract concept if you haven't lived/ learned them. Giving a quick response, helps learn a script to a problem occurring. This becomes a repeated narrative, which over time will be remembered as 'what to do'. We have to remember fraud, grooming and other exploitation of people online is because people are nice to you first, or something is appealing to us. When you have learning difficulties or disabilities you lack social maturity, and this increases your vulnerability. This is why we need to teach quick reflex responses to teach the skills, whilst the knowledge develops over time. Keeping communication open and frequent about what happens online, will give additional experience to apply quick reflexes and develop understanding of risks.	
Mission 15: **Warning! Warning! Advice video for all (how to report**	Following on from the previous session, film advice videos for quick reflexes as well as how to report harmful content	Pupils to recall rules. Starter: Pupils to recall the risks they found out form peers and TAs to support with presenting these back. Discuss most common risks and also the most significant risks.	This session will help you establish what is learned script from pupils and what they have actually done to manage risks. They might still be offer advice, even if they do not follow it themselves.	Warning! Warning! front page design templates

harmful content step by step)	I.e., Swearing, asking for personal details, getting cross, emergency	Main: Pick which risks you will make advice videos for, for pupils. Write a script and film. Make sure you cover rage, swearing, asking for and sharing personal details, inappropriate images. Where content is serious but too complex for pupils, chief agent must compile advice and send out to parents and put on the website. Plenary: Review videos and send agents away to design a front page for the videos. Chief agent will add the image and then share videos with all pupils. Special agents can also present videos in an assembly or to classes if appropriate.	It is important to cover emotions when online, because mental and physical health is very much impacted by time online. This should be one of the advice videos. It is important pupils are clear on moving and talking as much as possible.	
Mission 16: **Special Agents pen-pals**	Create a safe place for friends from other schools and meet other SEND pupils online	Pre-session preparation needed! You will need to find a school from the list in the resources section to link up with for pen pals. Starter: Discuss your partner school and the pupils there will be writing to you. You can use social media, emails, Teams etc. You will need to choose a platform between the two schools, so the format is clear and consistent for pupils. You could even plan a video call to introduce yourselves.	This mission will continue past this week's session as it is important the online friendships are authentic and positive. It is important you check what is being written and also empower parents to do this too. Your relationship and communication with the partner school is important to I've this the most impact. You may decide to set up online gaming tournaments or regular video calls to share information about what they have been doing or how the schools are different. This is a very positive expeirence of online	List of schools to have special agent pen pals

		Main: Script out what you might write to someone knew. It should be written or video content. You can script out what you will share and discuss the importance of consent. Link it back to digital personas and only sharing what you want to. Plenary: Send pupils away to contact their pen pal. Make sure parents are aware and you monitor the contact. Your TAs can also do this. It is important the contact is authentic and between peers to give the experience of positive online interaction with someone you haven't met before.	friendships, showing they can be very positive and safe. We are aiming to increase the positive online experiences so when someone negative does happen, pupils can spot it.	
Mission 17: **Online chat simulation**	Show behind the screens- working out who's who in chat and challenging bad language, highlighting warning bells of grooming etc.	Recall group rules. Pre-session preparation needed! You will need to set up a chat with evidence of positive and negative interactions on the most common forum your pupils use. Starter: Use a TA to simulate a real conversation with you on a screen and the pupils have to try and work out who is sending the messages. Then you can reveal the person. You should do this at least 3 times, at least once with a photo being sent a picture of a	This will help work out who can recognise when risks begin and help staff advise parents when they need to observe their child online. i.e., when they talk to everyone, or new people etc. This session is a good full class session and can be repeated regularly to give the lived experiences of pupils. It is important these screenshots replicate platforms the pupils use otherwise they will not be able to relate to it as it is too abstract.	Social media safe chat list Screenshot templates of chats

		face and it isn't that person- to highlight people lie online. Main: Share screenshots of different chats so pupils can try and find when things go wrong in the conversations. Recall the rules for when this happens. Make a list of who you can talk to if this happens and how to make yourself feel better (self-care tips.) Plenary: Compile self-care tips to share with all peers and add to the website. Create script for pupils to share with peers in class.	As part of this mission, it might be worthwhile creating a list of safe online chat apps. We know students enjoy talking to others on social media, so we should promote the safe environments in which this can happen.	
Mission 18: **Complete follow up pupil survey about school holidays**	To capture pupil online plans over the holidays and plan out what to do in the holidays for pupils – including hosting virtual enrichment sessions and what these should be based on	Recall rules led by pupils. Starter: Explain the next survey will be to help pupils over the holidays. Recall how the survey happened before and the best way to ask their peers how they do things online. This might need to go to parents as well as pupils if pupils cannot access the survey. Main: Plan out the questions and assign special agents to share the survey around school; they could email it or take a QR code round. Plenary:		Template survey

		TAs can support the survey being completed in school. You may want to film another quick introduction video to support completion of the survey.		
Mission 19: **Publish ‘what we do online’ presentation**	To create a summary of everything positive which happens online in the school community, showcasing with photos/ videos/ quotes- to promote positive online experiences within the community	Recall rules led by pupils. Starter: Ask pupils to list all the things we do online in the school and how we can show this. Pupils can then go and ask staff for the evidence so a full montage can be created. Main: Explain the montage of every we do and advice for the holidays will be linked together to inspire pupils and families to try something different if they are bored. Plenary: Chief agent will compile both pieces of work and share with special agents who then need to share around school and with parents.	It is important the use of technology and access to the interne tis promoted in this video to raise the confidence and digital awareness of parents. This in turn will increase pupil digital resilience because they will see all the positive things which will happen. Linking what happens in school and advice for the holidays will support parents navigating safe activities for their children to do over the holidays and give them more confidence when supervising online. Make sure you also add advice lines and reporting functions so parents feel safer on new website etc. Think of this as virtual handholding!	List of video making apps
Mission 20: **Write job description and advert for Special Agents**	To recognise the work completed to this point, and how important it is to work together. To summarise the purpose of the	Starter: Recall all the missions you have done this year and all the ways as a team you have supported pupils, parents and staff. Main:	It is important pupils celebrate the thing they have achieved and also can recall the learning from the missions. There is no reason why agents cannot stay on the team, but also agents can leave. It is	Template job description

based on the work they have done so far	group and welcome in new Special Agents.	Discuss the main skills you have needed and introduce the job description template to help find new special agents. Plenary: Special agents can share this with classes and staff. There should also be a section in the newsletter too.	important the agents involved are interested in being online.	

ONLINE SAFETY AND PUPIL WELLBEING

The Thrive framework is an essential framework for communities who are supporting the mental health and wellbeing of children, young people and their families.

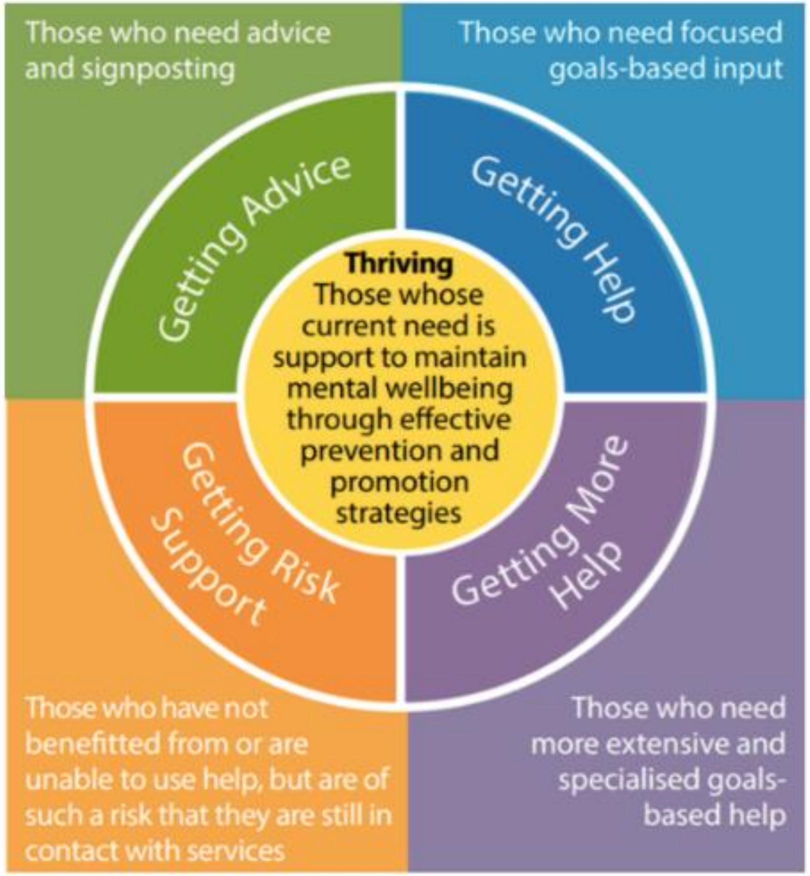
It aims to talk about mental health and mental health support in a common language that everyone understands. This has been proven to improve the support offered to children, young people and their families by different professionals as communication and efficiency is improved.

The framework is needs-led. This means mental health needs are defined by children, young people and families alongside professionals through shared decision making. Needs are not based on severity, diagnosis or health pathways.

Referenced: https://www.annafreud.org/mental-health-professionals/thrive-framework/

Social media and the internet can have both positive and negative effects on children and young people's mental health. Schools play an important role in educating pupils on how to stay safe online.

Research into the impact of internet and social media use on the mental health of young people is lacking. In a 2020 report, the Royal College of Psychiatrists called for more detailed and extensive studies in this area.



Those who need advice and signposting
Those who need focused goals-based input
Getting Advice
Getting Help
Thriving
Those whose current need is support to maintain mental wellbeing through effective prevention and promotion strategies
Getting Risk Support
Getting More Help
Those who have not benefitted from or are unable to use help, but are of such a risk that they are still in contact with services
Those who need more extensive and specialised goals-based help

A 2019 review from the government's Science and Technology Committee found that the majority of teenagers said that social media improved their relationships with their friends. However, the same report also highlights research stating that young people with a mental health disorder were more likely to use social media, and more likely to be on social media for longer.

To help you target support towards online safety concerns, we have categorised strategies, advice and guidance to support professionals working with pupils experiencing negative impacts on their mental health because of online activity.