Bryony School

E-Safety Policy

Bryony School identifies that the internet and information communication technologies are an important part of everyday life. Internet use is a statutory part of the curriculum and a necessary tool for staff and pupils. The school aims to provide pupils with quality Internet access as part of their learning experience.

The purpose of Bryony School's E-safety policy is to:

- Clearly identify the expectations of all members of the community with regards to the safe and responsible use of the schools' computer systems, the Internet and associated media and technology
- Safeguard and protect all members of Bryony School's community from harm online.
- Raise awareness regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy must be read in conjunction with the Acceptable Use of ICT Agreements other relevant school policies including (but not limited to) safeguarding and child protection, revised in line with Keeping Children Safe in Education, September 2022 and our Anti-bullying and Behaviour policies.

The Designated Safeguarding Lead (DSL) is Mrs Gee. The overall E-safety lead is Mrs Atkins. The Advisory Board will monitor the implementation of this policy. Mrs Harrison is the Advisory Board member responsible for Safeguarding.

This policy applies to:

- all **staff** including teachers, support staff, external contractors, visitors, volunteers and the Advisory Board members and other individuals who work for or provide services on behalf of the nursery, pre-school or main school (collectively referred to as 'staff' in this policy);
- all **children** in our Early Years, Key Stage 1 and Key Stage 2;
- all parents/carers of our children.

Responsibilities

All staff are responsible for following the Acceptable Use Agreements covering the use of ICT and Social Media. In addition to this are specific responsibilities listed below.

The key responsibilities of the Leadership team are:

- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including Acceptable Use of ICT Agreements.
- Ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content, which meet the needs of the school community whilst ensuring children have access to required educational material.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum, which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Having an awareness of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Ensuring there are robust reporting channels for the school to access regarding online safety concerns, including internal, local and national support.
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Overseeing the auditing and evaluation of online safety practice to identify strengths and areas for improvement.

The key responsibilities of the E-Safety Leads are:

- Acting as a named point of contact on all online safeguarding issues related to the Infant or Junior sites and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the Head teacher to ensure that data protection and data security practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken which are part of Bryony School’s safeguarding recording structures and mechanisms.
- Monitoring the school online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- Reporting to the school management team, the Advisory Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate such as our local PCSO and the NSPCC.
- Working with the Head teacher and management to review and update the online safety policies, Acceptable Use Agreements and other related policies at least annually.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

The key responsibilities for members of staff are:

- Teaching staff to complete the E-Safety training as part of the Bryony School training package.
- Taking responsibility for the security of school systems and data.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

The key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- Ensuring that suitable access controls and passwords as necessary are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Reporting any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Reporting any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

The key responsibilities of children and young people are:

- Adhering to the school Acceptable Use of ICT Agreement and Rules on use of ICT.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Contributing to the development of online safety policies at a level that is appropriate to their individual age, ability and vulnerabilities.

The key responsibilities of parents and carers are:

- Reading the school Acceptable Use of ICT and Social Media Agreement, E-Safety updates and encouraging their children to adhere to them, and adhering to them themselves where applicable.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.

- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Bryony School website

The school aims to keep the website up to date in line Department for Education (DfE) guidance. The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Business Manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

All school staff are responsible for ensuring that the use of images and videos take place in accordance with our safeguarding policy and Staff Code of Conduct. The school requests written permission from parents or carers for use of images, including for use of the school's website as part of the registration pack. Parents reserve the right to withdraw consent in writing at any time.

Appropriate and safe classroom use of the Internet

Internet use is an important feature of educational access and all children will receive age and ability appropriate education as part of curriculum requirements. Bryony School's Internet access is designed to enhance and extend education. All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential. At Bryony School, both computer rooms as designed so that all monitors are facing inwards towards teaching staff.

At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet is by adult demonstration with directly supervised programmes and access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school owned devices will be used in accordance with this E-Safety and ICT Acceptable Use Agreements and with appropriate safety and security measure in place. Members of staff will always evaluate websites, tools and apps fully before demonstrating them to pupils in the classroom or recommending them for use at home. The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

Official use of social media

Bryony School does not currently have an official social media presence such as Facebook or Twitter. Should we choose to do so in future as part of our communication with parents, this will be set up in line with the points below:

- Official use of social media sites by Bryony School will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Head teacher.
- Our official social media channel will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use Bryony School's email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy which will be revised accordingly to include written parental consent for use of images on social media sites.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites will be suitably protected (e.g. password protected)
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of Bryony School will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to Bryony School website to demonstrate that the account is official.
- Bryony School will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels by continuing to publish written newsletters for those that wish to have them.

Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and are in the Staff Code of Conduct. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of Bryony School's Acceptable Use Policy.

Staff should only use social media in their own time on their own devices. This must not be in the presence of children and be in line with the Staff Code of Conduct and Staff disciplinary Procedures.

Any concerns regarding the online conduct of any member of Bryony School community on social media sites should be reported to the Head teacher and will be managed in accordance with policies such as the Staff Disciplinary and Grievance Procedure, anti-bullying, behaviour and safeguarding/child protection policy. Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

Staff will not use personal social media accounts to make contact with pupils, nor should any contact be accepted. All members of staff are advised not to communicate with or add as 'friends' current or past pupils' family members via any personal social media sites, applications or profiles. However, the school recognises that this is not always possible, for example, given that some staff are also parents. In these cases, staff should consider restricting their privacy settings.

Members of staff will ensure that they do not represent their personal views as that of the school on social media. Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework. Members of staff will be encouraged to manage and control the content they share and post online. Advice is provided to staff via the National College online staff training course and by sharing appropriate guidance and resources on a regular basis.

Members of staff are encouraged not to identify themselves as employees of Bryony School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.

Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially should make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform the Designated Safeguarding Lead and/or the Head teacher, E-Safety Coordinators of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers related to the school through social media and will communicate via official communication channels.

- Staff using social media officially will sign the Bryony School social media Acceptable Use Policy.

Pupils use of social media by pupils

Pupils are not permitted to use social media sites at school. Any concerns regarding pupils' use of social networking, social media and personal publishing sites at home that are drawn to the attention of the school will be raised with parents/carers, particularly when concerning any underage use of social media sites.

The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School strongly encourages parents not to allow their child to create such an account.

Use of Personal Devices and Mobile Phones

Bryony School does not allow children to bring in mobile phones or any other electronic device into school. If a pupil needs to contact his/her parents/carers, staff may call the parent using the school phone and pass the phone to the child if appropriate. If a pupil is found with a phone or device, it will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with government guidelines:
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Staff use of personal devices and mobile phones

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose. Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. the Staff Code of Conduct and Acceptable Use.

Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times. Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the Bryony School Staff Grievance and Disciplinary Policy, Staff Code of Conduct and the procedure for managing allegations against staff.

Use of personal devices and mobile phones by Visitors

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy. Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy. The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Reducing online risks

Bryony School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The school currently uses an appropriate filtering system. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device. Therefore children are supervised whilst using the Internet as an additional preventative measure.

Internet use throughout the wider school

The school will provide an Acceptable Use Agreement for any guest/visitor who needs to access the school computer system or internet on site

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems. All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.

Engagement Approaches

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils. Education about safe and responsible use will precede internet access.

Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation. Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.

All users will be informed that network and Internet use will be monitored.

Online safety (e-Safety) will be included in the PSHE, Citizenship and Computing programmes of study, covering both safe school and home use.

Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between the Infant and Junior sites.

Acceptable Use expectations and Posters will be posted in all rooms with Internet access.

Engagement and education of children and young people considered to be vulnerable

Bryony School is aware that some children may be considered to be more vulnerable online due to a range of factors. Bryony School will ensure that differentiated and ability appropriate online safety (E-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Designated Safeguarding Lead)

Engagement and education of staff

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted in staff training days or staff meetings as part of our safeguarding responsibilities.

Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff via the National College and other staff briefings as appropriate.

All members of staff will be made aware via the Staff Code of Conduct that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Engagement and education of parents and carers

Bryony School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This includes a Safeguarding bulletin for parents with suggestions for safe home Internet use.

Managing Information Systems

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school is registered with the Information Commissioners Office (ICO) and this is renewed annually (April). Full information regarding the schools approach to data protection and information governance can be found in the schools confidentiality policy.

Security and Management of Information Systems

Virus protection will be updated regularly. Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via secure remote access systems.

Filtering and Monitoring

The Head teacher will ensure that the school has age and ability appropriate filtering and monitoring in place (SurfProtect) whilst using school devices and systems to limit children's exposure to online risks.

All users will be informed that use of school systems can be monitored to safeguard members of the community and that all monitoring will be in line with data protection, human rights and privacy legislation.

The school uses Surf Protect filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. It also blocks all sites on the Internet Watch Foundation (IWF) list. The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate. All changes to the school filtering policy will be logged and recorded.

All breaches of filtering must be reported to the Headteacher. If staff or pupils discover unsuitable sites, the URL will be reported to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead and will then be recorded and escalated as appropriate. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately. (www.ceop.police.uk/safety-centre)

Responding to Online Incidents and Safeguarding Concerns

All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This is highlighted in the National College training.

All members of Bryony School will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. The DSL will ensure that online safety concerns are escalated as necessary and reported to relevant agencies.

Any allegations against a member of staff's online conduct will be referred to the Medway LADO (Local Authority Designated Officer) by the DSL in line with the procedure outlined in Bryony School's Safeguarding Policy and Procedure.

Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure. The School's Complaints Policy and Procedure is available Pupils, parents and staff on the school's website. Hard copies are available on request.

The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Kent Police via 101 or 999 if there is immediate danger or risk of harm. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

Remote Learning

G Suite for Education enhances the way we teach and learn. Teaching staff and pupils have individual accounts. No personal information whatsoever, i.e. dates of birth, gender, addresses have been provided to Google.

During Lockdown from March 2020 due to the COVID-19 pandemic we were able to provide remote learning via Google Meet and upload classwork onto Google Classroom. This online facility is in place should we need to conduct remote learning again. Virtual learning is a key component of ensuring continuous learning during lockdown and our practice is in line with Keeping Children Safe in Education, September 2022.

Policy last reviewed	**September 2022** (to include reference to new KCSIE 2022 and continued reference to remote learning if needed)
To be reviewed	**September 2023**

Annex 1: *Procedures for Responding to Specific Online Incidents or Concerns*

Unsuitable Material unwittingly seen by a pupil

- *The pupil will have been taught to minimise the screen or turn off the screen and tell an adult*
- *The parents of the pupil will be informed.*
- *The adult with another adult witness will look at the page and note down the IP address. The E-Safety Coordinator will report the site to SurfProtect so that it cannot be accessed again.*
- *The incident will be logged in the school's E-Safety incident log.*

Indecent Images of Children (IIOC)

Bryony School will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises .The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example by implementing appropriate web filtering. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Medway Safeguarding Team or and/or Kent Police.

- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent and Medway Safeguarding Board procedures[1].
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
    - Ensure that the Designated Safeguard Lead 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.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
    - Ensure that the Designated Safeguard Lead 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 police via 101 (999 if there is an immediate risk of harm) and children's social services (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.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.

[1] http://www.proceduresonline.com/kentandmedway/chapters/p_ch_ab_tech.html

  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering and monitoring is in place with SurfProtect which has a filter in line with the PREVENT Duty guidance.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Medway Safeguarding Team and/or Kent Police.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of Bryony School will not be tolerated. There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by bullying including online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
  - Parent/carers of pupils involved in online bullying will be informed.
  - The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding online hate

- Online hate at Bryony School will not be tolerated. All incidents of online hate reported to the school will be recorded. The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Online Safety (e-Safety) Contacts and Resources

Kent Police:
www.kent.police.uk orwww.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Medway Safeguarding Children Board (KSCB): https://www.kscmp.org.uk/procedures/kent-and-medway-safeguarding-procedures

Kent e–Safety Blog: www.kentesafety.wordpress.com

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre):www.ceop.police.uk

ChildLine:www.childline.org.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

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Sexting:https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre:www.saferinternet.org.uk

360 Safe Self-Review Tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/