Gusford Primary School

Online Safety and Acceptable Use Policy 2017

The Active Learning Trust

Introduction
As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school/education setting or other establishments to ensure that children and young people are protected from potential harm both within and beyond the school/education setting or other establishment environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

'Safeguarding is not just about protecting children from deliberate harm. It relates to aspects of school life including Internet or e-safety.'
(Extract from Ofsted: Inspecting Safeguarding, September 2014)

Aims
Gusford identifies that the internet is an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school/education setting or other establishment .
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school/education setting or other establishment.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Writing and Reviewing the Online Policy
The policy has been approved and agreed by the Leadership/Management Team and governing body.
The School Online Safety Co-ordinator is Natalie Collins.
The School Designated Safeguarding Lead is Colin Tapscott and Marie Cridge.
The School Online Safety Lead for the Governing Body is…
The School Technician is Colette Bourne.
Policy approved by Governing Body: …
The date for the next policy review is…

Roles and Responsibilities

Governors & Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has a designated Online Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the school/education setting or other establishment.
- Time and resources is provided for the Online Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher/Online Safety Lead is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors at the Curriculum meetings about the progress of or any updates to the online safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding. At the Full Governor meetings, all Governors will be made aware of online safety developments from the Curriculum meetings.
- The Governors **MUST** ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.

- An Online Safety Governor (can be the ICT or Safeguarding Governor) will ensure the school has an Acceptable Use Policy (AUP) in place, with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT.
- Ensure that any misuse or incident is dealt with appropriately, according to policy and procedures (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police or involving parents/carers.

Online Safety Lead

It is the role of the designated Online Safety Lead to:

- Appreciate the importance of online safety within the school and to recognise that Gusford Primary has a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Reviewing and updating online safety policies, acceptable Use policies (AUPs) and other procedures on a regular basis.
- Ensure that staff have read the online safety policy and signed the AUP.
- Keeping up to date with current research, legislation and trends.
- Ensure training is available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Co-ordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanism.
- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Ensure that staff, governors and pupils have a good awareness of online safety and how to report any issues.
- Report issues and update the Headteacher on a regular basis.
- Ensuring that online safety is integrated with other appropriate school policies and procedures (PSHE and Safeguarding.)
- Ensuring the online safety is embedded within a progressive whole school curriculum which enables pupils to develop an age appropriate understanding of online safety and the associated risks and safe behaviours.
- Working alongside the technician to ensure the running and up keep of technology is in place for the curriculum.
- Encourage Peer Ambassadors, digital leaders, Online Safety Champions (or own title) within the school to provide peer to peer support around online issues.

Technician

It is the role of the Technician to:

- Taking responsibility for the implementation of safe security of systems.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform.
- Inform adults about the filtering levels and why they are there to protect children and young people.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported.
- Report any breaches or concerns to the Designated Safeguarding Lead and together ensure that they are recorded on the Online Safety Incident Log.

Staff and Adults

It is the responsibility of all adults within the school to:

- Contributing to the development of online safety policies and reading the AUPs and adhering to them.
- Having an awareness of online safety issues and how they relate to the children in their care.
- Embedding online safety education in the curriculum delivery wherever possible.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Report accidental access to inappropriate materials to the technician so that inappropriate sites are added to the restricted list or controlled with the Local Control options via your broadband connection.
- Ensure that they know who the Senior Designated Person for Safeguarding is within school/education setting or other establishment, so that any misuse or incidents can be reported which involve a child.
- Identifying individuals of concerns and taking appropriate action by working with the designated safeguarding lead.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Senior Designated Person immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Report incidents of inappropriate behaviour via the internet or other technologies using the Gusford incident log/ Pupil Asset.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged on.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

Children and Young People

Children and young people should be:

- Responsible for following the Acceptable Use Agreement whilst within the school setting as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Respecting the feelings and rights of others both on and offline.
- Taking responsibility for keeping themselves and others safe online.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Parents and Carers

It is the parent's role to:

- Read the AUP and encourage their child to adhere them and adhering to them themselves where appropriate.
- 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 new and emerging technology.
- Seeking help and support from school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Engagement and Education of Parents and Carers

Gusford Primary 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. A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent workshops with demonstrations and suggestions for safe home internet use or highlighting any online safety issues on our school website.

Online Communication and Safer Use of Technology

Filtering

Gusford Primary school uses a Draytek 2920 Router/Firewall with Web Content Filtering. Web-based content is filtered by the 3C Technology Ltd broadband connection with age appropriate settings. Changes can be made to the filtering levels through contact with 3C Technology Ltd.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department of Education.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school will post information about safeguarding, including online safety on the school website.

Publishing images and videos online

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school there is access to:

- Digital cameras
- Flip cameras
- iPads
- Netbooks
- Computers

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing. Photos taken on personal cameras and phones must be with the Headteacher's permission and downloaded onto a piece of school equipment e.g. laptop, network, or deleted within 2 weeks of being taken. Photos taken of children should be saved onto the school network. However, members of staff may have photos of children within documents stored on their laptops and stored accordingly.

The uploading of images to the school website should be subject to the same acceptable agreement as uploading to any personal online space. Permission will be sought from the parent/carer prior to the uploading of any images. Settings will consider which information is relevant to share with the general public on a website.

Managing email for staff

All members of staff are provided with a specific school/setting email address to use for any official communication.

- Any electronic communication which contains any content which could be subject to data protection legislation must be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- All staff school issued email addresses will include a standard disclaimer stating that the views expressed are not necessarily those of the Active Learning Trust.

Managing email for pupils

- Email addresses for children and young people to use, as a class and/or as individuals are part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.
- Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

- Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.
- Teachers are expected to monitor their class use of emails where there are communications between home and school.

Staff, children and young people should use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse.

Internet Use

Gusford Primary is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. However, due to the global and connected nature of internet content it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device but the school will take all reasonable precautions to ensure that users access only appropriate material.

Appropriate and safe classroom use of the Internet and associated devices

- The school's internet access will be designed to enhance and extend education.
- Pupils will use age and ability appropriate tools to search the internet for content.
- All children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- 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.
- Pupils will use age appropriate search engines and online tools when accessing materials online e.g. Safe Search kids.
- Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Appropriate and Inappropriate Use by Staff, Pupils and Parents

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

All staff, pupils and parents will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they will sign to be kept under file with a signed copy returned to the member of staff.
The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse. Also it is important to refer back to the Behaviour and Anti-Bullying Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs.

Should a child or young person be found to misuse the online facilities whilst at school/education setting or other establishment, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement will be reported, recorded and parents will be informed.
- Further misuse of the agreement will result in not being allowed to access the internet for a period of time and a meeting arranged with parents/carers to discuss the matter.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to minimise the window so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies will be addressed by the Online Safety Lead/Headteacher.

Responding to Online Incidents and Concerns

All members of the school/setting community will be informed about the procedure for reporting online safety concerns. The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded. The DSL will also ensure that online safety concerns are escalated and reported to relevant agencies.

Current Issues

There are a number of current issues that schools need to be particularly aware of. These include:

- Sexting- Is the act of sending sexually explicit messages or photographs, primarily between mobile phones.
- Sexual abuse online (including exploitation and grooming)
- Indecent images of children
- Radicalisation or extremism online
- Cyberbullying
- Trolling- Is when someone posts inflammatory messages in an online community, such as an online discussion forum, chat room or blog with the primary intent of provoking readers into an emotional response.

The Curriculum and Tools for Learning

Children will be taught how to use the internet safely and responsibly, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies will have been taught by the time they leave Year 6:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.
- If members of staff are participating in online activities they are requested to be professional at all times.

The teaching and learning online safety is embedded within the Computing curriculum (Switched On Computing e-Safety Road Map) to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence.

Pupils with Additional Learning Needs

Gusford Primary School provides access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Managing Social Media

Expectations regarding safe and responsible use of social media will apply to all members of Gusford Primary community and exist in order to safeguard both the school and wider community, on and offline. Examples of social media include blogs, wiki, social networking, forums, bulletin boards, online gaming, apps, videos/photo sharing sites, instant messenger and many others.

Advice for Staff

- Staff using social media will sign the Social Networking Policy.
- If members of staff are participating in online activities they are requested to be professional at all times.
- Social networking outside of work hours, on non-school issue equipment, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. See Social Network Policy for guidelines and advice given to staff.

Pupils

Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school acceptable use policy. Any concerns regarding pupil's use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with the parents/carers, particularly when concerning any underage use of social media sites.

Use of Personal Devices and Mobile Phones

Gusford Primary recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires such technologies need to be used safely and appropriately within school. Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items.

Pupils use

Children may bring their mobile phone into school, however, it will be taken to the office and secured away when the child arrives and given back to the child at the end of the school day.

Staff use

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- 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 and allegations will be responding to following the allegations management policy.

Managing Allegations against Adults Who Work With Children and Young People

Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Senior Designated Person (SDP) for safeguarding/Headteacher within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.