Glemsford Primary Academy
School Policy and Procedures
On-Line Safety
and Acceptable Use Policy

Date written / revised: October 2016

Revised: October 2017

Date approved by School Governors: October 2016

Signature of Chair of Governors:

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 Glemsford Primary Academy to ensure that children and young people are protected from potential harm both within and beyond the school setting. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

Aims

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 'e-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 the school setting.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or pupil, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school setting.
- 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.

Roles and Responsibilities

Governors and 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 pupils are aware of who takes this role within the school setting.
- Time and resources are 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 Learning and Achievement meetings about the progress of or any updates to the Online Safety curriculum (via PSHE or Computing) 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 L&A meeting.

- 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; proof of this should be fed back to the governors by the Online Safety Lead.
- An Online Safety Governor (can be the Computing 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, including:

Challenging the school about having:

- Firewalls.
- Anti-virus and anti-spyware software.
- Filters.
- Using an accredited ISP (internet Service Provider).
- Awareness of wireless technology issues.
- A clear policy on using personal devices.
- 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.

Local 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 Glemsford Primary Academy 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.
- Ensure that the AUP is reviewed annually, with up-to-date information and that 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 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 *or ensure the technician is informed and carries out work as directed*.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, safeguarding and Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified, in accordance with the Suffolk Safeguarding Children Board Allegations made Against Staff in Education Settings to ensure the correct procedures are used with incidents of misuse.

- Work alongside the technician, to ensure there is appropriate and up-to-date anti-virus software and antispyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- 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.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
  - Blanket e-mails are discouraged
  - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

Staff or Adults

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

- Ensure that they know who the Senior Designated Lead for Safeguarding is within the school, so that any misuse or incidents can be reported which involve a child. (DSL: Charlie Martin, DSL Alternate: Kelly Sorrell, Online Safety Lead: Suzanne Reeve and Safeguarding Governor Claire Martin.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Lead. 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 Lead immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Report any concerns regarding filtering levels to the Online Safety Coordinator.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- 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.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. 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 in.

- Report accidental access to inappropriate materials to the Online Safety Lead in order that inappropriate sites are added to the restricted list or controlled with the Local Control options via your broadband connection.
- 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'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.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the Glemsford Primary Academy accident/incident reporting procedure in the same way as for other non-physical assaults e.g. Logged on Glemsford Primary Academy Online Safety Incident Referral Form (see Appendix 7)

Children and Young People

Children and young people should be:

- Involved in the review of Acceptable Use Agreement in line with this policy being reviewed and updated.
- 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.
- Taught to use the internet in a safe and responsible manner through Computing, 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).

Appropriate and Inappropriate Use by Staff or Adults

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 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 the 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.

Please refer to appendices for a complete list of Acceptable Agreement for Staff.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet 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.

By Children or Young People

Acceptable Use Agreements are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within the school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The agreement will be on display within the classrooms, IT Suite and near stand alone PCs.

The school will encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreements are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond the school setting.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

Communications * with permission from the Headteacher following guidance outlined in this policy

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	* Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	●						●	
Use of mobile phones in lessons				●				●
Use of mobile phones in social time	●							●
Taking photos on school Ipads / cameras	●						●	
Use of other mobile devices eg tablets, Ipads			●				●	
Use of personal email addresses in school, or on school network	●							●
Use of school email for personal emails				●				●
Use of messaging apps			●					●
Use of social media				●				●
Use of blogs		●				●		

Inappropriate use

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					●
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					●
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					●
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					●
	Pornography				●	
	promotion of any kind of discrimination				●	
	threatening behaviour, including promotion of physical violence or mental harm				●	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				●	
Using school systems to run a private business					●	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					●	
Infringing copyright					●	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					●	
Creating or propagating computer viruses or other harmful files					●	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					●	
On-line gaming (educational)			●			
On-line gaming (non educational)					●	
On-line gambling					●	
On-line shopping / commerce					●	
File sharing			●			
Use of social media					●	
Use of messaging apps					●	
Use of video broadcasting eg Youtube					●	

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur

- Any child found to be misusing the internet by not following the Acceptable Use Agreement will have a letter sent home to parents/carers explaining the reason for suspending the child use for a particular lesson or activity.
- 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.

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.

The Curriculum and Tools for Learning

Internet Use

Children will be taught how to use the Internet safely and responsibly, through Computing 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.

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.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Images of children and young people should be stored according to policy.

Pupils with Additional Learning Needs

Glemsford Primary Academy 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.

Website

The uploading of images to the school website should be subject to the same acceptable use 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.

External Websites

In the event that a member of staff, or another adult, finds themselves on an external website, such as 'Rate My Teacher', as a victim, they are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

E-mail Use

E-mail 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.

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.

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.

Mobile Phones and Other Emerging Technologies

With permission, children may bring their mobile phone into school. However, it will be locked in the school safe when the child arrives and given back to the child at the end of the school day.

(I) Personal Mobile Devices

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.
- Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

(ii) School Issued Mobile Devices

The management of the use of these devices is similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop or Ipad, only this equipment should be used to conduct school business outside of the school building.

The children will be taught to understand the use of a public domain and the consequences of misuse. Relevant curriculum links will be made to highlight the legal implications and the involvement of law enforcement. Other technologies which the school use with children and young people include: Photocopiers, Telephones and IPads, Tablets and computers.

Video and Photographs

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
- iPads
- Flip cameras

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

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to the school website. Photographs should not include the child's first name.

The sharing of photographs via weblogs, forums or any other means online will only occur after permission has been given by a parent/carer or member of staff.

Managing Social Networking and Other Web Technologies

Staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, MySpace and Bebo.)

Glemsford Primary Academy does not allow access to social networking sites to be used on the school premises.

In response to this issue the following measures should be put in place:

- Pupils are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).
- Pupils are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school setting or uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.
- Pupils are reminded that some social networks have age restrictions.

Social Networking Advice for Staff

Social networking outside of work hours, is the personal choice of staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Head of School authorised systems (e.g. school email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- Any school social network sites used to manage and monitor public and pupil communications are to be managed by designated members of staff.

See Social Network Policy (Appendix 6)

Safeguarding Measures – Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.

Please refer to the Acceptable Use Agreement for Staff and children and young people for the appropriate use of the learning platform.

The E2BN broadband connectivity has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering is set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet. This also links to the E2BN criteria 'Schedule 11' of Level Four site filtering to qualify for access to the broadband services.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The Headteacher will sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from E2BN-pl. The levels listed below are in relation to age-appropriate categories:

Level One E2BN standard basic minimum adult policy.
Level Two E2BN standard senior pupils' policy.
Level Three E2BN standard younger pupils' policy.
Level Four E2BN standard young pupil's policy.
No search, no politics and religion.

This complies with the agreed connectivity legalities with Synetrix and E2BN and ensures our pupils are not exposed to unnecessary risks e.g. a blanket Level Two for Primary school users, is inappropriate.

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.

Children will use a search engine that is age appropriate such as Google Safesearch.

Links or feeds to Online Safety websites are provided.

Tools for Bypassing Filtering

Pupils and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

Note: Block banning of student's ICT or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

Monitoring

The Online Safety Lead/School Technician will monitor the use of online technologies by children and staff, on a regular basis. Network Managers do not have overall control of network monitoring.

Teachers will monitor the use of the Internet during lessons and also the use of e-mails from school and home, on a regular basis.

Computers around the school

All computers are protected in line with the network.
Where software is used that requires a child login, this is password protected so that the child is only able to access themselves as a user. Children and young people are taught not to share passwords. The same acceptable use agreement applies for any staff and children and young people using this technology, this will be displayed in all areas a computer is used.

Parents – Roles

Each child will receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement.

It is expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted. The school will keep a record of the signed forms.

Support

Parents too, have their part to play in keeping pupils safe and being aware of the school's policies. Interventions, for example, Family Learning workshops and courses on Online safety have a valuable part to play in the school's commitment to Online safety and acceptable use. These courses and workshops will be offered to parents/carers, offering the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond our school. The school wants to promote a positive attitude to using the World Wide Web and therefore wants parents to support their child's learning and understanding of how to use online technologies safely and responsibly. We will do this by holding an Online Safety Parent/Carer Information Evening once per annum, providing parents with information on how the school protects children and young people whilst using facilities, such as the Internet and E-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer 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.

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 Designated Safeguarding Lead (DSL) within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Designated Officer (known as 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.

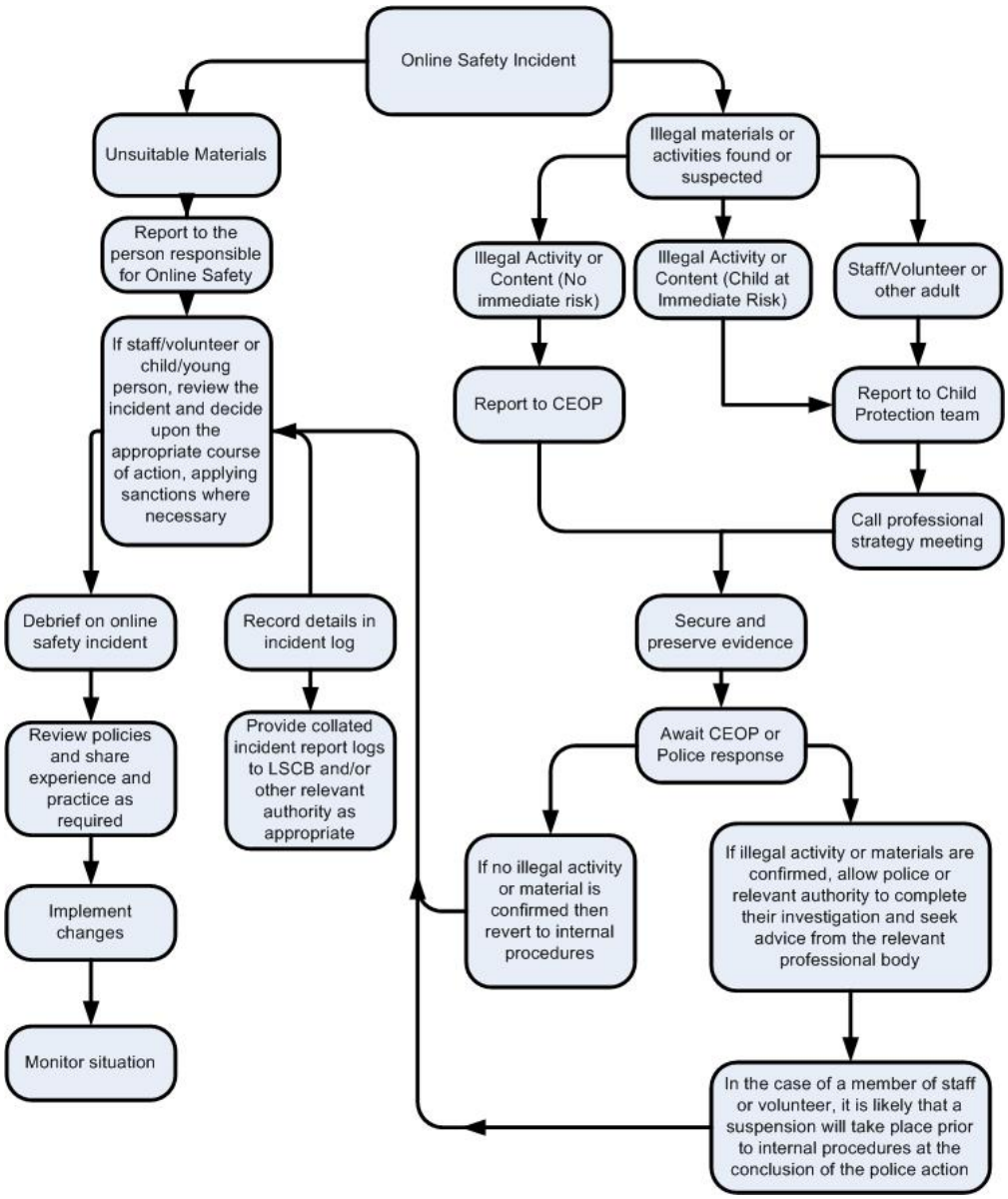
Disciplinary Procedure for All School/Education Setting or Other Establishment Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Curriculum Development

The teaching and learning of Online Safety is embedded within the PSHE and Computing curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line. A SCC Learning Together workshop for Year 6 Primary children is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible.

Appendix 1: Online Safety Flow Chart



Appendix 2

Acceptable Use Agreement for Staff and Governors

This agreement applies to all online use and to anything that may be downloaded or printed.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload/download images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of colleagues, children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or Online Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know that my Senior Designated Person is Charlie Martin, Senior Designated Alternative is Kelly Sorrell and Online Safety coordinator is Suzanne Reeve.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use my Glemsford Primary Academy e-mail address only to a child's Glemsford Primary e-mail address upon agreed use.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and recorded.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If someone requests my password I will check with the Online Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission to do so.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all Online Safety issues and procedures that I should follow.
- I will not use social networks on the school premises.

I have read, understood and agree with this Agreement as I know that by following it I have a better understanding of Online Safety and my responsibilities to safeguard myself, colleagues, children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

Appendix 3

Acceptable Use Agreement for Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or Online Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know that my Senior Designated Person is Charlie Martin, Senior Designated Alternative is Kelly Sorrell and Online Safety Coordinator is Suzanne Reeve.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If someone requests my password I will check with the Online Safety Coordinator prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software on a non-Glemsford Primary Academy issued device which I have permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Responsible Internet and Digital Technologies use document so I am clear on the procedures that I should follow.
- I will not use social network on the school premises.

I have read, understood and agree with this Agreement as I know that by following it I have a better understanding of Online Safety and my responsibilities to safeguard myself, colleagues, children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

Appendix 4 **Responsible Internet and Digital Technologies use**

Written: October 2016

Review date: October 2017

Communications * with permission from the Headteacher following guidance outlined in the Online Safety and Acceptable Use policy

	Staff & other adults				Pupils			
Communication Technologies	Allowed	owed at certain times	wed for selected staff	Not allowed	Allowed	owed at certain times	with staff permission	Not allowed
Mobile phones may be brought to school	●						●	
Use of mobile phones in lessons				●				●
Use of mobile phones in social time	●							●
Taking photos on school Ipads / cameras	●						●	
Use of other mobile devices eg tablets, Ipads			●				●	
Use of personal email addresses in school, or on school network	●							●
Use of school email for personal emails				●				●
Use of messaging apps			●					●
Use of social media				●				●
Use of blogs		●				●		

Inappropriate use

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					●
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					●
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					●
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					●
	Pornography				●	
	promotion of any kind of discrimination				●	
	threatening behaviour, including promotion of physical violence or mental harm				●	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				●	
Using school systems to run a private business					●	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					●	
Infringing copyright					●	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						
Creating or propagating computer viruses or other harmful files					●	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					●	
On-line gaming (educational)			●		●	
On-line gaming (non educational)					●	
On-line gambling					●	
On-line shopping / commerce					●	
File sharing			●			
Use of social media					●	
Use of messaging apps					●	
Use of video broadcasting eg Youtube					●	

Appendix 5 Example

Pupil Acceptable Use Agreement

My Online Safety Agreement

This is my agreement for using the internet safely and responsibly.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send electronic messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable or is not right, I know what to do.
- If I receive a message sent by someone I don't know, I know not to answer and what to do.
- I know I should follow these guidelines as part of the agreement with my teachers, parent or carer.
- I agree to look after myself and others by using my internet and electronic devices in a safe and responsible way.
- I understand that a member of Glemsford Primary Academy staff may confiscate my electronic device or restrict my internet access to keep myself and others safe or if I do not act in accordance with this agreement.

Signed (Child) ..... Dated.....

Name.....(Printed)

I will help my child to always use the internet in a safe and responsible way.

Signed (Parent/Carer)..... Dated.....

Name.....(Printed)

Appendix 6

Introduction

Social Networking through internet sites such as Facebook has become more and more popular over the last few years. The vast majority of staff at Glemsford Primary Academy now have Facebook accounts. Many parents and many children, some as young as 7, also have accounts. A number of problems have occurred in Suffolk schools recently where staff have inadvertently made a comment or posted a photo/video that has led to parental complaints. This puts the Governors and Senior Managers in the school in a very difficult position and the member of staff may face disciplinary action for unprofessional conduct. The following list of Do's and Don'ts is an attempt to protect staff from such action.

DO

- Select your "friends" carefully and consider who is able to see your profile – remember that friends of your friends may sit with them at a computer or may be given access without you knowing.
- Limit access to your profile to only your "friends"; ensure that your privacy settings are always up to date
  -the social networking providers change the setup of these frequently.
- Update privacy settings every 3 months to avoid default settings being used by the social network group resetting your privacy settings.
- Ensure that the privacy settings on your photo albums are set to "friends only".
- Ensure comments/photos/videos of yourself that may be posted by you or others do not show you or other members of staff in a way that could be construed as unprofessional for a member of staff/volunteer working in a school.
- Consider carefully the "groups" that you may join and are then shown on your profile.
- Use language that is appropriate as a member of Glemsford Primary Academy.
- Consider carefully comments made on any social network medium will reflect on you and the school

DO NOT

- Accept children (under the age of 18) that you have met/taught in the course of your profession as "friends".
- Upload photos/videos of school activities that involve children or jeopardise the professional status of others.
- Post any comments of any nature about children and/or parents in the school.
- Post any comments or pictures about staff or school activities

Please note that privacy and security settings are not guaranteed and that anything you post may become in the public domain. Any breach of the above may result in disciplinary action.

Name:

Signed: Date:

Appendix 7

Online Safety Incident Referral Form

Date:	Name of referrer:		Role:	
Glemsford Primary Academy		Tel: 01787 283200		
Details of incident:				
Who referred to:	Name:	Signed:	Date:	Time:
Is a child or young person involved?				
Yes – Is this a Child Protection issue? (explain)		No – (explain)		
Action taken:				
Who referred to:	Name:	Signed:	Date:	Time: