GREAT FINBOROUGH CHURCH PRIMARY

Online Safety & Acceptable Use Policy

Linked documents:
Safeguarding Policy
Child Protection Procedures
Information Management Policy
Data Protection Policy

Prepared by:	H Elliss
Date Last Reviewed:	September 2018
Chair of Governors:	Jamie Warner
Chair of Committee:	Neil Watts
Minuted:	Pending

Acknowledgement: This policy has been developed using the SWGfL Online Safety template policies

Table of Contents

Contents

Introduction

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about online safety incidents and monitoring reports. The Safeguarding Governor also has responsibility for the oversight of online safety.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive periodic monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets periodically with the Online Safety Governor to discuss current issues, and review incident logs
- reports as required to Senior Leadership Team
- monitoring incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision

Technical staff:

The Business Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- All systems use the Smoothwall proxy server to enable filtering and adult and child settings are applied to systems as appropriate
- that the email addresses used by pupils are monitored for inappropriate content

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and Online Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use wherever possible and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

should be aware of online safety issues and the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Volunteers

Volunteers who access school systems as part of the wider school provision will be expected to sign the Staff and Volunteer AUA before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through appropriate activities and literature.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Internet access is via the schools' broadband service provided by School's Choice and the service is monitored by the Schools Choice network team. School staff will liaise with them as necessary. The school will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be a review and audit of the safety and security of school technical systems when there are major system changes
- Servers, wireless systems and cabling is securely located
- All users will have clearly defined access rights to school technical systems and devices.
- The "master / administrator" passwords for the school ICT system, used by the Business Manager are also be available to the Headteacher and kept in the school safe
- The Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installation
- Internet access is filtered for all users. Illegal content is filtered by Smoothwall the filtering provider
- The school has provided differentiated user-level filtering for staff and pupils
- School technical staff reserve the right to monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Any actual or potential technical incident / security breach should be reported to the Headteacher and the Business Manager.
- Wireless encryption is used on all Access Points.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary access for "guests" eg trainee teachers, supply teachers, and visitors into the school systems may be granted via the 'Teacher' user on school laptops.
- Staff issued with laptops that may be taken home should only use them for work related activities, use of eBay, Facebook, developing personal websites, or activities related to a commercial business outside school are not allowed.
- Staff should only download executable files and install programmes on school devices with the agreement of the Business Manager (or Headteacher in her absence).
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by GDPR and the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images must not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. In the event that it is necessary to use a personal device, the business manager or online safety co-ordinator should be notified, a log of the details made, and the images transferred to a school system and removed from the personal device as soon as possible.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR and the Data Protection Act 2018 which state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

See the *Data Protection* and *Information Management Policies*.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies - personal devices	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	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones / cameras (only when no school device is available)		X						X
Use of other mobile devices eg tablets, for work purposes only	X					X		
Use of personal email addresses in school, or on school network			X					X
Use of school email for personal emails				X				X
Use of messaging apps – for school purposes only		X					X	
Use of social media – for school purposes only		X					X	
Use of blogs – for school purposes only		X					X	

When using communication technologies the school considers the following as good practice:

- Should be aware that email communications may be monitored. Staff and pupils should therefore use only the school email service to communicate with others on school business.

- Users must immediately report, to the Headteacher or Business Manager in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses or social media must not be used for these communications. In certain circumstances, e.g.,on school trips, text messaging is permitted, but the school text messaging system should be used in preference wherever possible.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff or governors.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school does not currently use social media for professional purposes.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

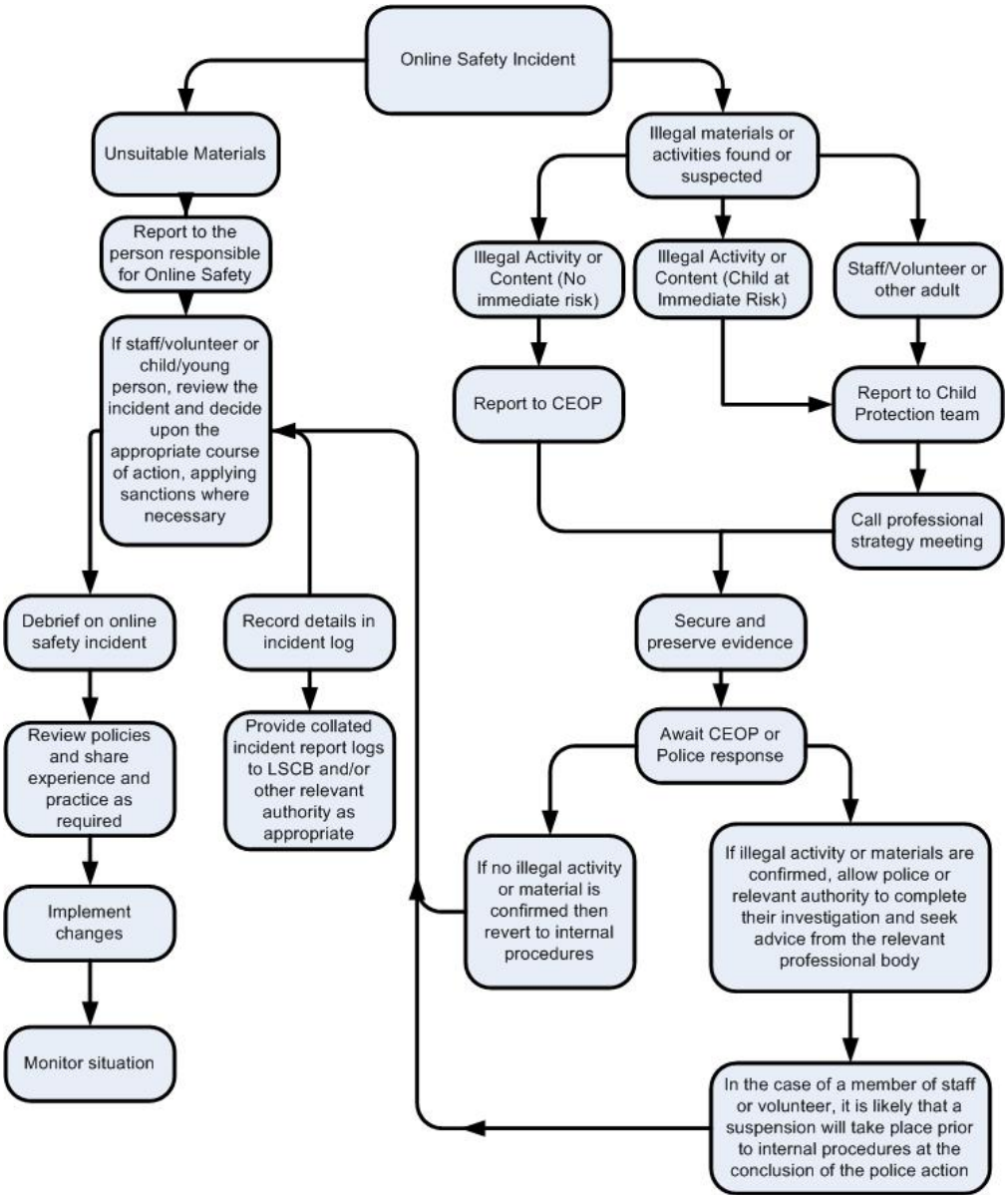
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child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

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

Incidents:	Refer to class teacher	Refer to technical support staff for action re filtering / security etc	Refer to Headteacher	Inform parents / carers	Removal of network / internet access rights	Warning		Further sanction eg detention / exclusion	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X						X
Unauthorised use of non-educational sites during lessons	X		X						
Unauthorised use of mobile phone / digital camera / other mobile device	X		X						
Unauthorised use of social media / messaging apps / personal email	X	X	X						
Unauthorised downloading or uploading of files	X	X	X						
Allowing others to access school network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school network, using another student's / pupil's account	X		X						
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X						
Corrupting or destroying the data of other users	X	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X						
Continued infringements of the above, following previous warnings or sanctions				X	X	X		X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X		X				
Using proxy sites or other means to subvert the school's filtering system	X	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X				X	
Receipt or transmission of material that infringes the copyright of another person or infringes GDPR or the Data Protection Act 2018	X		X	X	X	X		X	

Staff

Incidents:	Refer to Headteacher	Refer to Technical Support Staff for action re filtering etc	Refer to HR	Warning	Suspension	Disciplinary action	Refer to Local Authority / HR	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X				X	X
Inappropriate personal use of the internet / social media / personal email	X		X					
Unauthorised downloading or uploading of files	X	X	X	X				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X	X				
Careless use of personal data eg holding or transferring data in an insecure manner	X		X	X				
Deliberate actions to breach data protection or network security rules	X		X	X				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X		X		X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X		X		X		X	
Actions which could compromise the staff member's professional standing	X		X	X				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X	X				
Using proxy sites or other means to subvert the school's 's filtering system	X	x	X	X	X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X				
Deliberately accessing or trying to access offensive or pornographic material	X	x	X		X		X	
Breaching copyright or licensing regulations	X		X	X				
Continued infringements of the above, following previous warnings or sanctions	X				X	X		

School Policy on Acceptable Use

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Appendices

Can be found on the following pages:

Pupil Acceptable Use Agreement – for older pupils (KS2)

I understand that I must use school laptops and tablets in a responsible way, to ensure make sure that I am safe and I keep others safe

- I understand that the school will monitor my use of school computers.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (e.g., my name, home address or school))m
- I will only speak to people online with the Teacher's permission.
- I will immediately report anything I see or hear online that makes me uncomfortable.
- I understand that school computers are for school use and I will not use them to play games, or access anything online not related to school work without permission from a teacher
- I will respect others' work and property and will not copy, delete or change anyone else's work unless I have their permission.
- I will be polite and responsible when I communicate with others online.
- I will not take or post images of anyone online without their permission.
- I will not use my own mobile phone, tablet or laptop in school without permission from a teacher.
- I will not try to success anything on the internet that is unsuitable for my age.
- I will immediately report any damage or faults involving school computers even if was the cause of the damage.
- I will not open emails or any attachments to emails, unless I know and trust the person who sent the email.
- I will not attempt to install programmes on any school computer, nor will I try to alter any computer settings.
- I will only use social media sites with permission and at the times that are allowed.
- When I am using the internet to find information, I wil be aware that the information may not be accurate and should be checked.
- I will not directly copy anyone else's work from the internet
- I will not threaten or otherwise bully anyone online whether in school or out of school.
- I understand that if I break any part of this agreement I may not be allowed to use school computers and my parents will be informed..

I have read and understand the acceptable use agreement and agree to follow these guidelines when:

- I use the school computers and when I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, website etc.

Name of Pupil

Signed

Date

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent): ……..

Staff and Volunteer Acceptable Use Agreement

Great Finborough Church Primary understands that the use of technology for teaching and learning has great. It can allow work to be completed more efficiently by pupils, broaden the kinds of tasks they can undertake, enrich and enliven lessons and offers scope for creativity, differentiation and stretch. The School takes all reasonable steps to ensure safe internet access at all times, but all colleagues must use the internet safely and responsibly within their professional lives. Additionally, teaching and non-teaching colleagues must use the internet and social media in accordance with the Teachers' Standards.

Great Finborough Church Primary expects that all colleagues will behave responsibly, with courtesy and sensitivity to others at all times, including when using technology. Colleagues are required to act in line with the Code of Conduct and this agreement.

Digital technologies have become integral to society, both within schools and outside of them. These technologies are powerful tools, which open up new opportunities for everyone. They can inform, promote creativity and effective learning. They bring opportunities for staff to be better informed and more productive in their working environment.

This ICT Acceptable Use Agreement for staff and volunteers is intended to ensure that, as far as is reasonably practicable,

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Terms of the Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I understand that this is important because this could result in a data breach which would render the school liable to a fine.
- If another person (e.g., supply teacher) needs to use my laptop, I will give them the password for the Supply user on my laptop, or ask the Business Manager for a new user to be set up.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only use an email address issued by the school, using a school domain name, for communication with parents/carers or when conducting school business with third parties. Any such communication will be professional in tone and manner.
- I will only communicate with parents / carers using a personal 'phone if allowed by the Headteacher.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this has been agreed with the Business Manager
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as allowed by Data Protection. Where digital personal data is to be transferred outside the secure local network, it must be encrypted (the school office have and Egress email address for use when secure transfer by encrypted email is required). Paper-based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

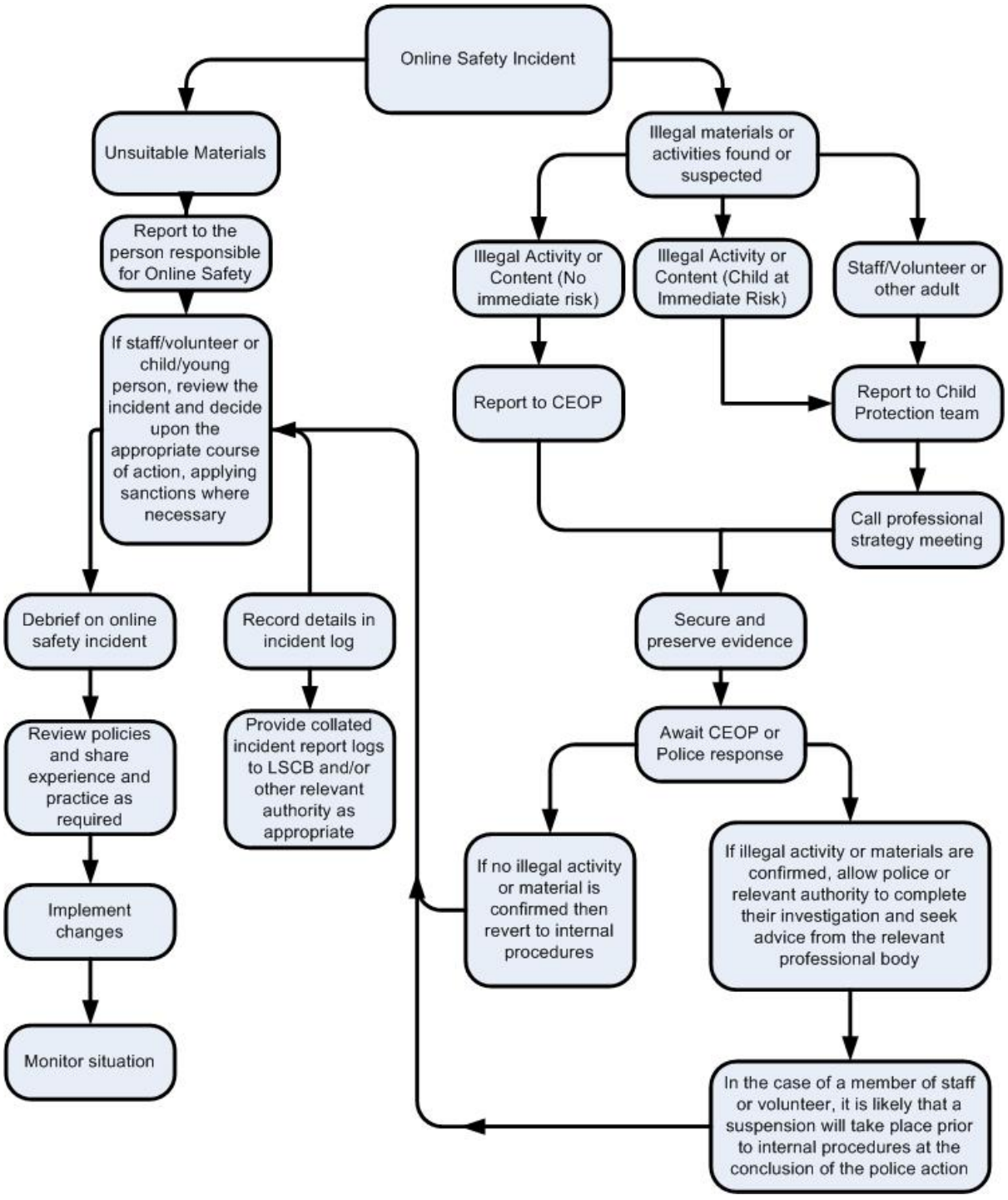
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Template Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident		Signature
			What?	By whom?	Reported by		