SIR THOMAS BOTELER
CHURCH OF ENGLAND HIGH SCHOOL
THROUGH GOD, WE CARE

GRAMMAR SCHOOL ROAD
LATCHFORD, WARRINGTON
WA4 1JL
01925 636414
01925 417468
INFO@BOTELER.ORG.UK
WWW.BOTELER.ORG.UK
/THOMASBOTELER
#THOMASBOTELER

Diocese of Liverpool
THE CHURCH OF ENGLAND Diocese of Chester

E-SAFETY POLICY

AUTHOR:	Mr M Frodsham
COMMITTEE:	Headteacher
AUDIENCE:	Students, Staff, Governing Body, Parents/Carers
PUBLISHED:	VLE, School Website
UPDATED:	12th March 2020
DATE OF REVIEW:	As required

Contents

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Therefore, it is essential to have an e-safety policy. Where we use the terms 'e-safety' or 'online', we refer to all fixed and mobile technologies which children and young people might encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety.

Scope of the Policy

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety Co-ordinator.
- The Headteacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see WBC flow chart 'Responding to incidents of misuse' in Appendix 1.1)

Designated e-safety Coordinator:

The designated e-safety Coordinator is Mr M Frodsham.

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- reports regularly to Senior Leadership Team

Business Manager/Technical staff:

The Business Manager is responsible for ensuring:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- virus protection will be installed and updated regularly.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the e-safety Co-ordinator for investigation/action/sanction
- digital communications with pupils (email/VLE) should be on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other school activities

Designated Person for Child Protection/Designated Safeguarding Lead (DSL):

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

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

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which is available on the Desktop of all school machines
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- may only use approved e-mail accounts on the school system.
- must immediately tell a teacher if they receive offensive e-mail.
- must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school.

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. e-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT/PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Education & Training – Staff and Governors

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. A planned programme of formal e-safety training will be made available to staff.

- An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- Governors should take part in e-safety training/awareness

Technical

- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password to access the school network and VLE.
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff passwords are changed every 100 days.

Curriculum

- e-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- e-safety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- e-safety skills should be embedded through both discrete ICT and cross-curricular application.
- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited.

Use of Digital and Video Images

- 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 e.g. on social networking sites.
- Digital images/video should only be captured on school owned equipment.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site, in line with GDPR regulations.

- Work can only be published with the permission of the pupil and parents, in line with GDPR regulations.

Social Networking

Social Networking has become an accepted way of communication both personally and professionally. Apart from concerns over the corporate image of Sir Thomas Boteler Church of England High School, we also need to take extra precautions due to working in a school.

The use of social networking sites is allowed/permitted in school, if they have not been blocked by internet filtering, but this should not detract from your day to day tasks.

There are also the obvious safeguarding concerns with regards to employee and pupil communication that this policy also addresses.

Social Networking Sites.

There are an increasing number of social networking sites, and this policy is intended to cover **all** social networking sites, not just Facebook, Twitter and LinkedIn. The general use of YouTube (watching videos) is not included in this policy, but all other aspects of YouTube are included.

Corporate Image.

It is common practice to include your place of work in your profile. This helps identify your colleagues on social networking sites, and can also be used to promote Sir Thomas Boteler, however if employees decide to include Sir Thomas Boteler they are to some extent a representative of Sir Thomas Boteler Church and therefore items that are posted by its representatives can reflect on the image of Sir Thomas Boteler.

It should be understood by all employees that if requested by either the Business Manager or Headteacher, to remove Sir Thomas Boteler from their profile they will do so immediately.

Confidential Information.

Confidential information about Sir Thomas Boteler, or one of its employees or pupils should under **no circumstances** be posted on social networking sites, including private messages that are available on some sites.

Pupil Interaction

Under **no circumstances** should a current pupil be linked to your social networks. It is recommended that you do not add ex-pupils.

If a pupil sends a request to be an employee's 'friend' the employee must ignore and decline the request and inform the e-safety coordinator, the safeguarding officer or the DSL.

If there is an educational purpose to interact with pupils on social networking sites employees must ensure that the Business Manager and/or Headteacher are fully aware of the activity.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018. Please refer to the GDPR Policy.

Managing Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-safety Coordinator or the Business Manager.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Communications

- Users need to be aware that all that network and Internet use will be monitored.
- Users must immediately report, to the e-safety Coordinator the receipt of any email that makes them feel uncomfortable is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the table title 'Acceptable uses of the system' (see Appendix 1.1) would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage.

Reasonable Precautions

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WBC can accept liability for the material accessed, or any consequences of Internet access.

Responding to Incidents of Misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If this is found to be the case then the flow chart titled 'Dealing with e-safety incidents' (see Appendix 1.2) should be followed.

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 in line with the Behaviour Policy. The form titled 'Recording incidents of misuse - Pupils' (see Appendix 1.3) should be used to record misuse.

Legislation

Schools should be aware of the legislative framework under which this e-safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

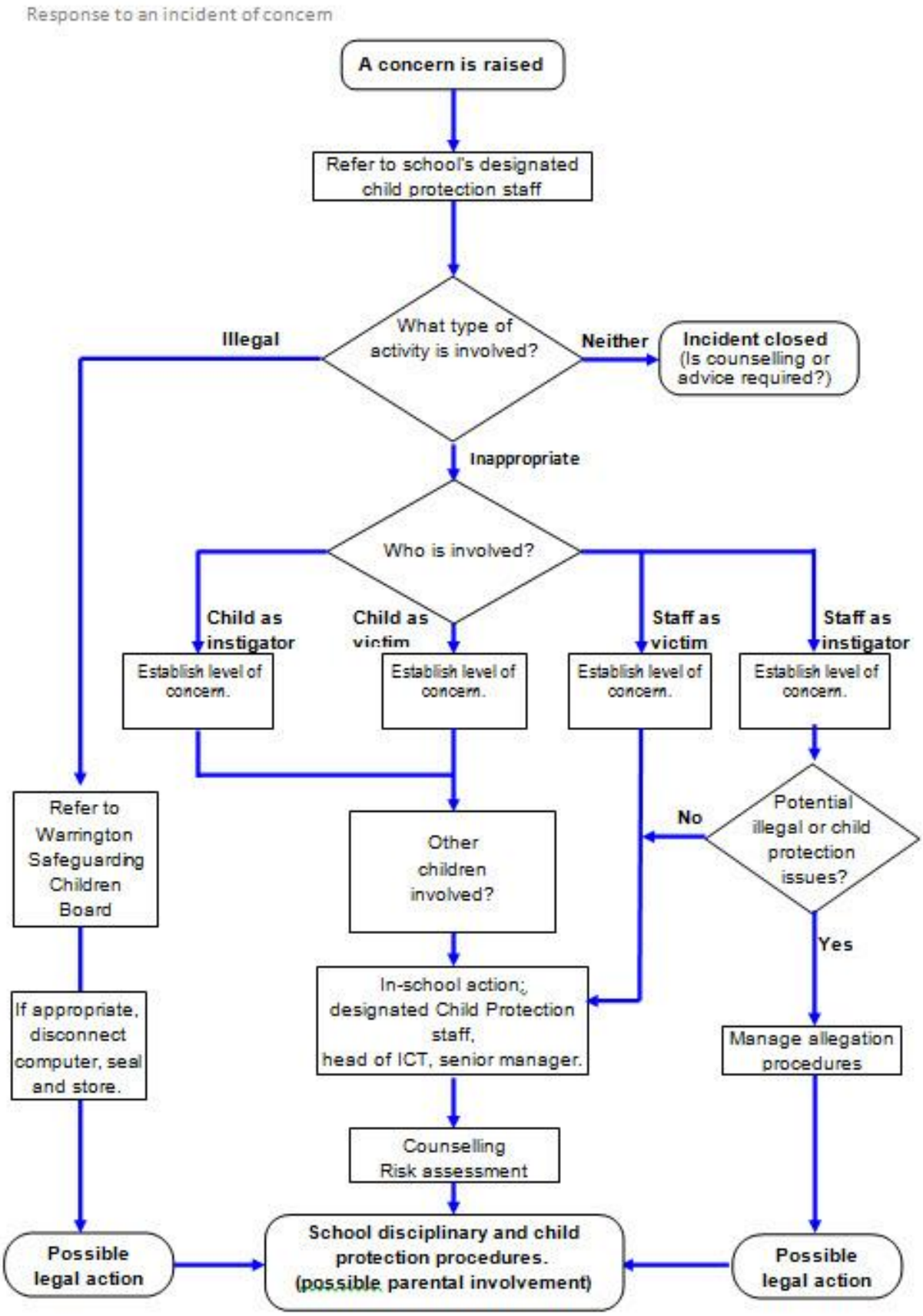
Linked documents: GDPR Policy, Behaviour Policy, Acceptable Use Policy, Disciplinary Procedures, Monitoring Procedures, Anti-Bullying Policy, Child Protection/Safeguarding Policy,

Appendix 1.1 - Acceptable uses of the system

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				✓	✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓	✓
	criminally racist material in UK				✓	✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	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					✓	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by WBC and/or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
Online gaming (educational)	✓				
Online gaming (non-educational)		✓			
Online gambling				✓	
Online shopping/commerce		✓			
File sharing				✓	
Use of social networking sites		✓			
Use of video broadcasting e.g. YouTube	✓				

Appendix 1.2 - Dealing with e-safety incidents



Appendix 1.3 – Recording incidents of misuse – students

Pupils Actions/Sanctions

Incidents:	Refer to class teacher/ tutor	Refer to Head of Department /Head of Year/other	Refer to Head teacher	Refer to Police	Refer to technical support staff for actioner filtering/security etc.	Inform parents /carers	Removal of network/ internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone/digital camera/other handheld device									
Unauthorised use of social networking/instant messaging/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									

Attempting to access or accessing the school network, using another student's/pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									

Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulations 2018 (GDPR)									

Appendix 1.4 – Recording incidents of misuse - staff

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority/ HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).								
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email								
Unauthorised downloading or uploading of files								
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								
Careless use of personal data e.g. holding or transferring data in an insecure manner								

Deliberate actions to breach data protection (GDPR) or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature								
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								

Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								