Battledown Centre for Children & Families

A Specialist Early Years Centre

E-Safety

This Policy also links with the Safeguarding Policy and should be read in conjunction.

This policy covers all aspects of school's work including Special School, Extended Services (inc Daycare) and Child Development Centre

Committee Responsible: Safeguarding & Premises

Date of Policy: July 2017

Review Date: July 2018

Signed: R Sutton
Chair of Governors

Date: 17th July 2017

1. Introduction

Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils. Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online. School will not accept responsibility for any content that has not been accessed through the school network.

At Battledown we understand the responsibility to protect and educate our school community where appropriate in relation to E-Safety issues; providing training, knowledge and understanding to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, plasma screens, digital video equipment, etc.)

This policy applies to all staff and authorised users who bring their own computers/ digital equipment into Battledown - whether they connect them to the school network or not.

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.

2. Roles and Responsibilities

E-Safety is an important aspect of strategic leadership within school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2.1 Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Safeguarding and Premises Committee in their receiving regular information about e-safety incidents and monitoring reports.

Governors will maintain an up to date awareness of e-safety matters and of the current school e-safety policy and practices

Governors will read, understand and sign the school Staff Acceptable Use Policy / Agreement (AUP) and report any suspected misuse or problem to the Headteacher for investigation / action / sanction

2.2 Headteacher

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 is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and E- Safety Co-ordinator are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

2.3 E-Safety Coordinator

The named E-Safety co-ordinator is the Business Administrator and it is her role to keep abreast of current issues and guidance through relevant organisations, reporting back the Senior Leadership Team and staff meetings.

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- provides training, advice for staff together with procedures and changes.
- liaises with the School Business Manager, Local Authority and SWGfL to ensure the school's ICT infrastructure is secure and continues to meets the needs of the school reporting to Governor Safeguarding & Premises Committee and Senior Leadership Team

2.4 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 and signed the school Staff Acceptable Use Policy / Agreement (AUP) and report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- digital communications should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities adapted to meet the young/complex needs of the children.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and they monitor their use and follow the procedures set to these devices.
- in class where internet use is pre-planned staff should ensure sites are checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2.5 Designated Safeguarding Lead (DSL)

The named DSL is the Headteacher and the deputies are the Deputy Headteacher and Business Manager. They are aware of the potential for serious child protection issues to arise from e-safety issues:

- sharing of personal data

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

3. Education & Training

Staff, students and volunteers

- It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. Staff are made aware of the school's password policy at Induction and through the E-Safety policy and Acceptable Use Agreement.
- Staff receive regular information and training on E-Safety issues in the form of staff/team meetings, INSET days and notices.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

Governors

Governors are invited to take part INSET days and training/awareness sessions. This is offered in a number of ways, via:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school information sessions for staff or parents.
- Information sharing at the Governors' Safeguarding and Premises Committee

Parents/Carers and Wider Community

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:

- Curriculum activities
- Letters, newsletters, website
- Parents/Carers INFOCUS sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
- The school website will provide online safety information for the wider community

4. Infrastructure, Security, Filtering & Monitoring

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Internet access is filtered for all users. Illegal content (child sexual abuse images) is controlled through the managed filtering service provided by SWGfL at an enhanced level to ensure the need to manually filter is not required.
- Where access to a specific website is required by staff, the website is un-filtered via the SWGfL custom filtering policies. The Headteacher and E- Safety Co-ordinator have access to the staff proxy server.
- Battledown is aware of its responsibility when monitoring staff communication under current legislation and staff are made aware that school based email and internet activity can be monitored and explored further if required.
- Staff are not permitted to download/upload programs or files on school based technologies.
- The school's wireless network is protected by a password.
- The school infrastructure and individual workstations are protected by up to date virus software. Virus protection is purchased through our Microsoft Volume Licensing Agreement with SWGfL. Anti-Virus software is installed on all compatible school devices and updated regularly.
- Users are made responsible for the security of their username and password. They 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 to the Headteacher/E-Safety Co-ordinator.
- Pupils only access on-line materials with supervision of staff members due to their age and ability and are therefore not allocated passwords.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks which includes following Data Protection guidelines when accessing school data.
- The school has set up google alerts linked to the school name and employed staff.

5. Managing the Internet/Email

- Staff will preview any recommended sites before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources i.e Google images.
- All accounts are password protected to ensure that the contents are adequately secured and computers should be logged off after use to prevent logon sharing.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Users must immediately report, to the Headteacher/E-safety co-ordinator in accordance with the school policy, 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.

Privacy and Monitoring:

Understandably, staff and authorised users wish for the contents of their own computers, their network user accounts and their webmail accounts to be confidential and private. However, the school must be allowed to monitor and regulate activity on all computers, which are used within Battledown, in order to ensure that nothing of an inappropriate nature is held or accessed. This is of paramount importance in a school environment. Suspicious material will be investigated and logged. The log will be kept by the Headteacher.

6. Social Networking and Personal Publishing

- The school will block/filter access to open social networking sites and give access only to those sites that are monitored and approved by SWGfL recommendations.
- Due to the age/complex needs of Battledown children, we share information about the potential risks of social networking sites and what information should not be shared on such sites.
- Staff should not provide details or information of their own, or any other person or pupil on internet sites that could relate to Battledown. This includes all social media, web blogs, forums or chat rooms e.g. Facebook, Twitter, etc. Exceptions should be checked with the Headteacher.
- School staff are made aware that they must not accept invitations from pupils or parents/carers of children at Battledown to join their social network. Parents/Carers who make such invitations will be informed of the school policies. Staff should be wary of adding pupils or parents/carers who have recently left the school to their social network as they may provide an indirect link to current children or parents/carers.
- Personal use of mobile devices during recreation time is acceptable provided that staff are not accessing personal social networking sites in places in school where children, parents/carers or professionals can see the screen and content.
- Staff receive regular briefings regrading online safety and professional etiquette.
- The Headteacher and E-Safety Coordinator manage the School Facebook Page and Twitter account. They respond to social media comments made by others.
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- Staff are advised if they use snapchat to turn snapmap onto ghost mode whilst at school, this will ensure that contacts don't know the staff members precise location and their actions.

7. Mobile devices (including phones)

The school allows staff/visitors to bring in personal mobile phones and devices for their own use. These are not permitted to be used in the presence of children except in an emergency when using the school mobile.

Anyone who hasn't read and signed the Acceptable User agreement (this includes Student/Volunteers/ Parents/Governors/Visitors) is required to leave their mobile device in reception during their time in school. The exception to this being during recreation time in the staff room.

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not permitted.
- No images or sound recordings are permitted to be made on these devices by any member of the school community.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops for offsite visits and trips, only these devices should be used to conduct school business inside/outside of school.

8. Safe Use of Images

The development of digital imaging technologies has created significant benefits to learning, allowing the instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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:
We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the following:

- Written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with **only** school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils.
- Images taken on school provided devices should be transferred immediately and solely to the school's network and deleted from the device.

Publishing Pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school website including Facebook and Twitter.
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states 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.

Battledown will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Images/ films of children are stored on the School computer network.
- Class teachers are responsible for deleting the images when they are no longer required, or the pupil has left the school.

9. School Website

Battledown Centre for Children & Families values the contribution that a school website can make towards:- providing information for and communication between:

- Parents of existing pupils
- Parents of prospective pupils
- The larger community outside of the school
- Staff and pupils

assisting with raising standards in

- Teaching and learning
- Self esteem

promoting

- The values, aims and philosophy of the school
- The achievements of pupils

Site Administration
Provision of materials for the site is undertaken by the identified link members of staff. Contributions from all staff, governors, parents and pupils are given to the Business Administrator in an electronic format on a regular basis to enable the site to be kept up to date.

Materials must only be uploaded to the site once they have been checked and approved by the **Web Administrator** who has access to all areas of the website. This role is undertaken by the Business Administrator who has responsibility to liaise with SMT for the overall content of the site.

Site Safety
It is the duty of the school to ensure that every child in its care is safe. The same principles apply to the virtual presence of the school as much as to the physical presence. The school will seek to ensure that no pupil can be identified or contacted either via or as a result of using the school website.

Pupil Involvement
Pupils who are able to understand the request will be asked whether they are happy for their images or work to be put on the website before this material is added.

Maintenance of the Site
The school website will be monitored and updated regularly to ensure that it complies with the rules stated above.

10. Voxer

Clear guidelines about using Voxer are distributed to parents before they sign up to use the App. Staff must also read and follow the guidance.

11. Misuse and Infringements

12.1 Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and 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 as follows:

User Actions		Acceptable	Unacceptable
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	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		✓

to:	Pornography	▨	✓
	Promotion of any kind of discrimination	▨	✓
	Promotion of extremism or terrorism	▨	✓
	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 SWGfL and / or the school		▨	✓
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		▨	✓
On-line gambling		▨	✓
On-line shopping / commerce for educational purposes		✓	
On-line shopping / commerce for non-educational during recreation/break times		✓	
Use of messaging apps as a communication aid i.e Voxer		✓	
Use of social networking sites on school systems, except for school Facebook Page		▨	✓
Use of video broadcasting e.g. Youtube		▨	✓

12.2 Complaints

Complaints relating to E-Safety should be made to the Headteacher, logged and responded to by following the **Flowcharts for incidents of misuse.** (see next page)

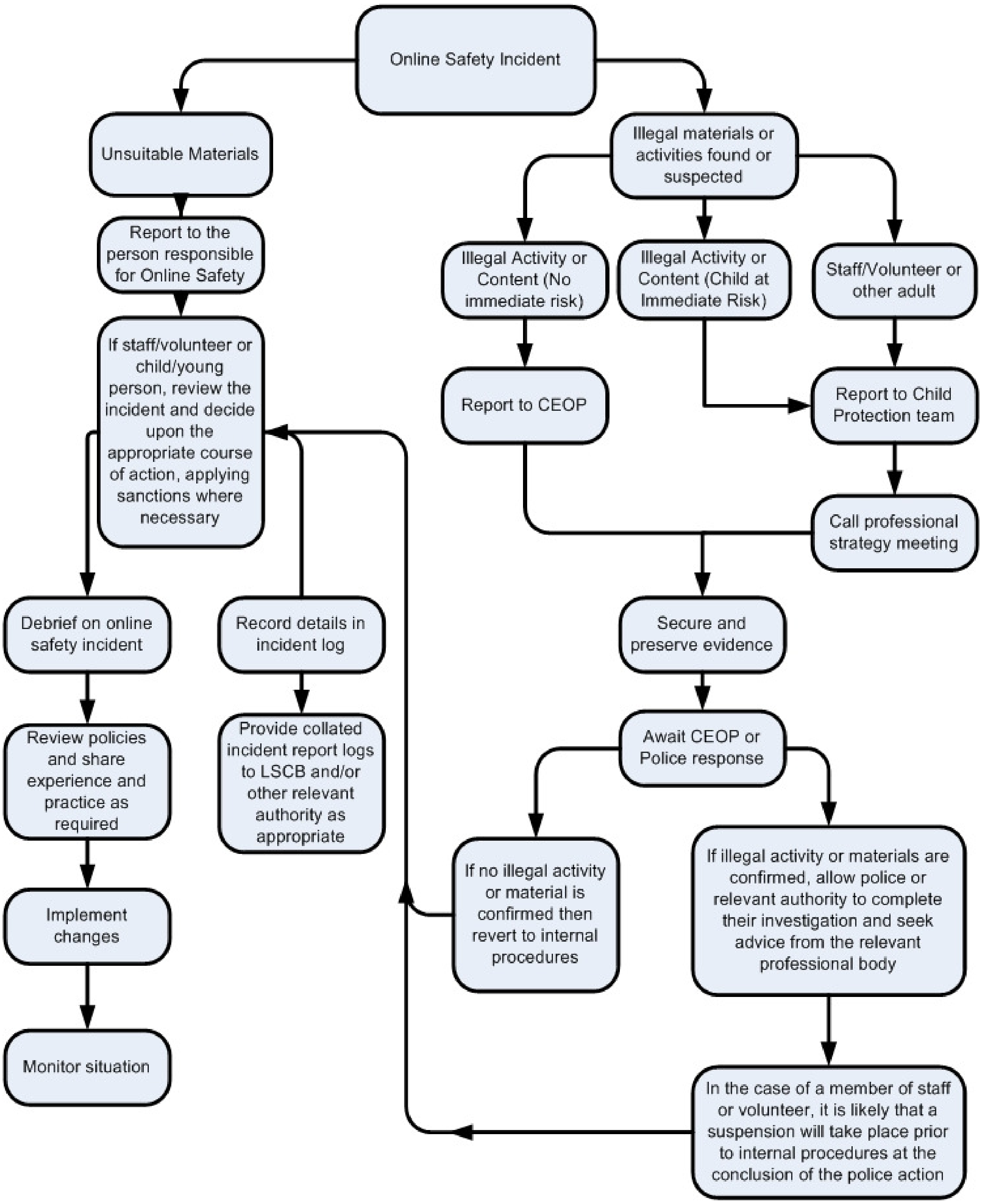
12.3 Sanctions

Staff and authorised users who breach this will have their user accounts and/or webmail accounts disabled, pending further investigation by the Headteacher. Staff and authorised users computers may also be confiscated whilst investigations take place.

12.4 Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

IT Monitoring and Security incidents Log

Monitoring Activity	
Security Incident/breach	

Date of review or Incident	
Reviewed by:	

Details
Action taken
Reported to:
Signed by Headteacher:
Signed by Chair of Governors: