**Twiss Green**

**eSafety Policy**

Content

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities

* Governors
* Headteacher and Senior Leaders
* eSafety Co-ordinator
* ICT Coordinator/Technical Staff
* Teaching and Support Staff
* Designated Person for Child Protection
* eSafety Committee
* Pupils
* Parents/Carers
* Community Users

Policy Statements

* Education – Pupils
* Education – Parents/Carers
* Education – Extended Schools
* Education and training – Staff
* Training – Governors
* Technical – infrastructure/equipment, filtering and monitoring
* Curriculum
* Use of digital and video images
* Data protection
* Communications
* Unsuitable/inappropriate activities
* Responding to incidents of misuse

Development, Monitoring, Review of this Policy

4

This eSafety policy has been developed through consultation with:

* School eSafety Coordinator (Headteacher)
* Senior Leaders
* Teachers
* Support Staff
* ICT Technical staff
* Governors
* Parents and Carers

Consultation with the whole school community has taken place through the following:

* Staff meetings
* School Council
* Governors meeting/committee meeting
* Parents’ evening
* School website/newsletters

Schedule for Development, Monitoring, Review

5

|  |  |
| --- | --- |
| This eSafety policy was approved by the Governing Body/Governors Sub Committee on: | Nov 2017 |
| The implementation of this eSafety policy will be monitored by the: | eSafety Coordinator |
| Monitoring will take place at regular intervals: | annually |
| The Governing Body/Governors Sub Committee will receive a report on the implementation of the eSafety policy generated by the monitoring group (which will include anonymous details of eSafety incidents) at regular intervals: | annually |
| The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place. The next anticipated review date will be: | Nov 2019Reviewed 10/9/19 following query regarding pupil and staff password policies. |
| Should serious eSafety incidents take place, the following external persons/ agencies should be informed: | LA ICT Manager, LA Safeguarding Officer, Police  |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Surveys/questionnaires of

• pupils (eg Ofsted “Tell-us” survey/CEOP ThinkUknow survey)

• parents/carers

• staff

6

Scope of the Policy

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 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 eSafety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 eSafety behaviour that take place out of school.

Roles and Responsibilities

7

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/ Learning Community Sub Committee receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

* regular meetings with the designated eSafety Co-ordinator
* regular monitoring of eSafety incident logs
* regular monitoring of filtering/change control logs
* reporting to relevant Governors committee/meeting

Headteacher and Senior Leaders:

* **The Headteacher is responsible for ensuring the safety (including eSafety) of members of the school community**.
* The Headteacher is responsible for ensuring that the eSafety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
* The eSafety Coordinator will be supported by a designated eSafety Governor and report logged incidents to them. This will include an annual report on eSafety to the Governing Body.
* **The Headteacher and 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 eSafety allegation being made against a member of staff.** (see WBC flow chart on dealing with eSafety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures)

Designated eSafety Coordinator:

8

* takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
* provides training and advice for staff
* liaises with the Local Authority
* liaises with school ICT technical staff
* receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments,
* meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering/change control logs
* attends relevant meeting/committee of Governors
* reports regularly to Senior Leadership Team

Network Manager/Technical staff:

The ICT Co-ordinator is responsible for ensuring:

* **that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack**
* **that the school meets the eSafety technical requirements as advised by Becta and the Acceptable Use Policy.**
* that he/she keeps up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant.
* that the use of the Learning Platform and other communication technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the eSafety Co-ordinator for investigation.

9

Teaching and Support Staff

are responsible for ensuring that:

* **they have an up to date awareness of eSafety matters and of the current school eSafety policy and practices**
* **they have read, understood and signed the school Staff Acceptable Use Policy**
* **they report any suspected misuse or problem to the eSafety Co-ordinator for investigation.**
* **digital communications with pupils (Learning Platform) should be on a professional level**.
* pupils understand and follow the school eSafety and acceptable use policy
* pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. This should be made clear in all year groups, but especially so in year groups where research and homework are more likely to involve breach of copyright.
* they monitor ICT activity in lessons, extra curricular and extended school activities
* they are aware of eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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 and that processes are in place for dealing with any unsuitable material that is found in internet searches. Search terms should be limited to those that the teacher has previously checked the first two pages of results. Teachers may use a search engine in lessons at the request of pupils, but must do so independently of the pupils.

Designated person for child protection/Child Protection Officer

should be trained in eSafety 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

10

Pupils:

* **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.**(at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* should report abuse, misuse or access to inappropriate materials to a member of staff as soon as possible.
* 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 eSafety practice when using digital technologies out of school and realise that the school’s eSafety 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, Learning Platform and information about national/local eSafety campaigns/literature. Parents and carers will be responsible for:

* **endorsing (by signature) the Student/Pupil Acceptable Use Policy**
* accessing the school Learning Platform in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems/Learning Platform as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

11

Policy Statements

Passwords – pupils (October ’19)

All passwords used by children for educational purposes, as directed by the school, should be communicated to parents in a sealed envelope via the standard form. Pupil passwords will be stored in a spreadsheet maintained on Google Drive (protected by staff password). Staff may access the password file only to update changed passwords, or to facilitate learning in the event of the pupil ‘forgetting’ their password.

Passwords – Staff (October ’19)

Members of staff should not divulge their school passwords to anyone and should take all reasonable steps to use strong passwords. If a member of staff suspects that their password is compromised, it should be changed at the earliest opportunity.

Google Drive (October ’19)

Files stored in the organisation ‘twissgreen.net’ should always be protected with a strong password, changed annually. Where files are to be shared, they should be shared only with those that need access and never ‘outside of the organisation’. Only allocated ‘twissgreen.net’ accounts may be used to create, store, access, or share files. Members of staff that have personal Google (or other) accounts should ensure that they are not logged into such when using the ‘twissgreen.net’ drive.

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 eSafety is therefore an essential part of the school’s eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience.eSafety education will be provided in the following ways:

* **A planned eSafety programme should be provided as part of PSHEE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.**
* **Key eSafety messages will be reinforced as part of a planned programme of assemblies.**
* **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 student/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
* Rules for use of ICT systems/internet will be posted in all rooms
* Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children’s online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, and theLearning Platform
* Parents’ evenings
* Reference to the WGfL website

Education & Training – Staff

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

* **A planned programme of formal eSafety training will be made available to staff. An audit of the eSafety training needs of all staff will be carried out regularly.** It is expected that some staff will identify eSafety as a training need within the performance management process.
* **All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies**
* The eSafety Coordinator will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/WBC and others.
* This eSafety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.

Training – Governors

**Governors should take part in eSafety training/awareness sessions**, with particular importance for those who are members of any committee/group involved in ICT/eSafety/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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafety responsibilities:**

* **School ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined by Becta and the Acceptable Usage Policy**
* **School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smartboard should be updated regularly.**
* **There will be regular reviews and audits of the safety and security of school ICT systems.**
* **Servers, wireless systems and cabling must be securely located and physical access restricted.**

13

* **All users will have clearly defined access rights to school ICT systems.**
* **All userswill be provided with a username and password to access the school network**by the ICT Coordinator. Group usernames are acceptable for class use.
* **All users of the school learning platform will be provided with a username and password for secure access in school and beyond.**
* **The “master/administrator” passwords for the school ICT system, used by the ICT Coordinator and technician must also be available to the Headteacher.**
* **School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.**
* The school maintains and supports the managed filtering service provided by Warrington Borough Council.
* In the event of the ICT Coordinator or technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
* Any filtering issues should be reported immediately to Warrington’s IT support on 2200.
* Requests from staff for sites to be added or removed from the filtered list will be considered by the eSafety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the eSafety Committee
* ‘Guests’(eg. Trainee teachers, DBS cleared adults, etc) will use a separate username and password to log on to the school system.

14

* An agreement is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school. This includes the installation of software and changes to administrative settings.

Curriculum

**eSafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.**

* **eSafety should be taught regularly through PSHEE with identified progression of knowledge, skills and understanding.**
* **eSafety 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.
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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.**

15

* Members of staff 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.
* 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.
* Students’/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. This forms part of the ‘Home/School Agreement’.

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:(GDPR to be incorporated -6.11.18)

* 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.

**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.**

When personal data is stored on any portable computer system, USB stick or any other removable media:

* the data must be encrypted and password protected
* the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
* the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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(outside of those available on the learning platform) | Allowed | Allowed |
| Mobile phones may be brought to school | YES | NO, unless agreed with a parent/carer and retained during school hours by Class Teacher/Office |
| Use of mobile phones in lessons | For administrative school reasons only. | NO |
| Use of mobile phones in social time | YES | NO |
| Taking photos on mobile phones or other camera devices | Not on personal devices. | Only as part of planned lessons |
| Use of hand held devices eg netbooks, PDAs, PSPs, iPad, iPod | YES | Only as part of planned lessons |
| Use of personal email addresses in school, or on school network | YES | NO |
| Use of school email for personal emails | NO | NO |
| Use of chat rooms/facilities | Only as part of planned lessons | Only as part of planned lessons / homework |
| Use of instant messaging  | Only as part of planned lessons | Only as part of planned lessons |
| Use of social networking sites | NO | NO |
| Use of blogs  | Only educational/professional activities. | YES, but only those held on the school Learning Platform |

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

* **Where available the official school email service may be regarded as safe and secure and is monitored.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
* **Users need to be aware that email communications may be monitored**
* **Users must immediately report, to the nominated person – 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.**
* **Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platformetc) must be professional in tone and content.**

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 certain internet usage as follows:

18

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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, eg 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 (eg 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 eg YouTube**19 |  | ✓ |  |  |  |

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 any apparent or actual misuse appears to involve illegal activity ie.**
* **child sexual abuse images**
* **adult material which potentially breaches the Obscene Publications Act**
* **criminally racist material**
* **other criminal conduct, activity or materials**

**theWBC flow chart – below and should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.**



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

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. All of the following MUST be reported to the Headteacher as soon as practicable:

|  |
| --- |
| Pupils |
| Incidents: |
| **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 Data Protection Act |

|  |
| --- |
| Staff |
| Incidents: |
| **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 eg holding or transferring data in an insecure manner |
| Deliberate actions to breach data protection 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 |