

2

St Patrick’s & St Joseph’s Primary School

E-Safety Policy

**Development / Monitoring / Review of this Policy**

4

This e-safety policy has been developed by a working group made up of:

*• Principal / Senior Leaders*

*• E-Safety Officer / Coordinator*

*• Staff – including Teachers, Support Staff*

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This e-safety policy was approved by the *Governors Sub Committee on:* |  |
| The implementation of this e-safety policy will be monitored by the: | *the E-Safety Coordinator Mr Morrow* |
| Monitoring will take place in conjunction with the Pastoral Care & Discipline, Anti–Bullying and Safe Guarding Children policies at regular intervals: | *During the first academic term* |
| The E-Safety Policy will, in conjunction with the Pastoral Care & Discipline, Anti–Bullying and Safe Guarding Children policies be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *September 2018*  *Next full review due 2019/20* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Chairman of the Board of Governors, C2k and the Police* |

The school will monitor the impact of the policy using:

*• Logs of reported incidents*

*• Surveys / questionnaires on a three year basis by means of*

*• students / pupils*

*•* parents / carers

*• staff*

*(ICT coordinator to devise simple questionnaire for each group. Questionnaires to be submitted with each full review – next due 2019/20.)*

6

**Scope of the Policy**

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

The schoolwill 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 e-safety behaviour that take place out of school.

**Roles and Responsibilities**

7

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

**Governors / Board of Directors:**

*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* receiving an annual report about e-safety incidents and monitoring reports.

**Principal and Senior Leaders:**

• **The *Principal* has a duty of care 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 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 flow chart on dealing with e-safety incidents.

*• The Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*

**E-Safety Coordinator / Officer:**

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies

• 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 Education Authority and C2k

• receives reports of e-safety incidents, informs principal of these immediately and creates a log of incidents to inform future e-safety developments,

**Staff:**

**It is school policy that all:**

**• users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**

• staff keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

**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 Staff Acceptable Use Policy**

**• they report any suspected misuse or problem to the *Principal, E-Safety Coordinator***

**• all digital communications with students / pupils / parents / carers should be on a professional level** *and only carried out using official school systems*

• e-safety issues are embedded in most aspects of the curriculum and other activities

• students / pupils understand and follow the e-safety and acceptable use policies

• 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 students / pupils should be guided to sites checked as suitable for their use. Pupils will be instructed to immediately close any sites where they feel unsuitable material has occurred and to report the incident. Staff will inform the principal who will in turn inform C2k.*

**Child Protection / Safeguarding Designated Person / Officer**

should be trained in e-safety issues and be aware of 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

Students / pupils:

**• are responsible for using the *school / academy* digital technology systems in accordance with the Student / Pupil Acceptable Use Policy**

• have a good understanding of research skills

• 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 i.e. no personal devices allowed in school capable of accessing the internet. They should also know and understand 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.

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 through *parents’ newsletters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

**•** digital and video images taken at school events

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-safety is therefore an essential part of the school’s e-safety provision. 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 should be a focus in most areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

**• Key e-safety messages should be reinforced as part of a planned programme of assemblies or tutorial / pastoral activities**

**• Students / 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.**

**• Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**

*• Students / pupils should be helped to understand the need for the student / 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 students / 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.*

*• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that C2k can temporarily remove those sites from the filtered list for the period of study. Any request to do so, must have the principal’s permission, with clear reasons for the need.*

Education – parents / carers

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

*• Curriculum activities*

*• Newsletters, web site*

*• High profile events / campaigns eg Safer Internet Day*

*• Reference to the relevant web sites / publications eg* [*www.swgfl.org.uk*](http://www.swgfl.org.uk)[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers> (see appendix for further links / resources)

Education & Training – Staff / Volunteers

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

• **A planned programme of formal e-safety training will be made available to staff. This will be updated and reinforced annually with the safe guarding children training. 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 Agreements.**

*• The E-Safety Coordinator / Officer will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*

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 to report any areas of concern to the principal

**• All users will have clearly defined access rights to school devices.**

• **All users** (at KS2 and above) **will be provided with a username and secure password** by *the school secretary who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password when requested by C2K.* (Schools / Academies may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the associated risks – see appendix)

*•* **Internet access is filtered for all users by C2k.**

• The provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems is provided by the secretary in the form of a guest logon and password.

*• Staff are forbidden from downloading executable files and installing programmes on school devices.*

*• Staff are permitted to use removable media (e.g. memory sticks / CDs / DVDs) on school devices providing they only contain work related to the school. DVD’s or photographs are only to be used or stored for school uses in line with parental consent and never to be put on social media sites.*

**Bring Your Own Device (BYOD)**

Currently no devices are allowed in school.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils 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 cyber bullying 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 students / 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.**

•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 in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / 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.*

• *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*

• *Students / pupils must not take, use, share, publish or distribute images of others without their permission*

• *Photographs published on the website, or elsewhere that include students / 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.*

• *Consent will be requested from parents or carers at the beginning of the child’s career in the school for photographs of pupils/ pupils’ work to be published on the school website , school Facebook , and school twitter sites via the Data Collection form (Appendix 1).*

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.

**The school must 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.**
* **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
* Responsible persons are appointed – the principal and the secretary
* It has clear and understood arrangements for the security, storage and transfer of personal data
* Data subjects have rights of access and there are clear procedures for this to be obtained
* There are clear and understood policies and routines for the deletion and disposal of data

**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.**

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** | Not allowed | Allowed | Allowed at certain times | Not allowed | Allowed |
| Mobile phones may be brought into school |  | ✓ |  | x |  |
| Use of mobile phones in lessons | x |  |  | x |  |
| Use of mobile phones in social time |  | ✓ |  | x |  |
| Taking photos on mobile phones / cameras |  |  | ✓ | x |  |
| Use of other mobile devices eg tablets, gaming devices | 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 | x |  |  | x |  |
| Use of social media | x |  |  | x |  |
| Use of blogs | x |  |  | x |  |

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

**• The official *school* service may be regarded as safe and secure and is monitored.****Users should be aware that email communications are monitored by C2k.**  *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school (eg by remote access).*

**• Users must immediately report, to the nominated person – in accordance with the school / academy 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.** (SWGfL BOOST includes an anonymous reporting app Whisper -<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper>**)**

**• Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE (Virtual Learning Environment) etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*

*• Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school / academy email addresses for educational use.*

*• Students / pupils should be taught about e-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.*

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/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

* Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>)
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk

School staff should ensure that:

* No reference should be made in social media to students / 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 /academy* or local authority

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  18 | | 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 / academy** | |  |  |  | X |  |
| **Infringing copyright** | |  |  |  | X |  |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | |  |  |  | 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)** | |  | ✓ |  |  |  |
| **On-line gaming (non educational)** | |  |  |  | x |  |
| **On-line gambling** | |  |  |  | x |  |
| **On-line shopping / commerce** | |  | ✓ |  |  |  |
| **File sharing** | |  |  |  | x |  |
| **Use of social media** | |  |  |  | x |  |
| **Use of messaging apps** | |  |  |  | x |  |
| **Use of video broadcasting eg Youtube**  19 | |  | ✓ |  |  |  |

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). SWGfL BOOST includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when managing reported incidents (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool>)

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.**

|  |  |  |
| --- | --- | --- |
| **ONLINE SAFETY INCIDENT** | | |
| ↙ |  | ↘ |
| Unsuitable material | Illegal Material |
| ↓ | ↓ |
| Secure and preserve evidence  do not permit any other user to use the machine/ask for possession of the device | Secure and preserve evidence  Do not permit any other user into the room where incident occurred/ask for possession of the device |
| ↓ | ↓ |
| Inform principal | Inform principal |
| ↓ | ↓ |
| Seek advice from C2k, SWGFL and if incident concerns a child the Safe Guarding Team in the Antrim Board Centre | Seek advice from CCMS, C2k, SWGFL and if incident concerns a child the Safe Guarding Team in the Antrim Board Centre  Inform PSNI/ Chair of Board of Governors |
| ↓ | ↓ |
| Decide, where appropriate, sanctions | Decide, where appropriate, sanctions |
| ↓ | ↓ |
| Record incident on C2k system | Record incident on C2k system |
|  |  |

School / Academy Actions & Sanctions

It is more likely that the school / academy 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

|  |
| --- |
| Students / Pupils |
| Incidents: | Refer to class teacher / tutor | Refer to Principal | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
| **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 | X |
| Unauthorised use of non-educational sites during lessons |  | X |  |  | X |  | X |  |
| Unauthorised use of mobile phone / digital camera / other mobile device |  | X |  |  | 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 / academy network by sharing username and passwords | X |  |  |  | X |  | X |  |
| Attempting to access or accessing the school / academy network, using another student’s / pupil’s account |  | X |  |  | X |  | X |  |
| Attempting to access or accessing the school / academy 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 |  |
| 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 / academy’s filtering system |  | 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 |  |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 |  | X |  |  | X |  | X |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Staff | Actions / Sanctions | | | | | | | | | |
| Incidents: | | Refer to Chair of Governors | Refer to Principal | Refer to EA / C2k | 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).** | | X | X | X | X |  |  | X | X |
| Inappropriate personal use of the internet / social media / 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 or attempting to access or accessing the school network, using another person’s account | | 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 |  |  |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | | X | X |  |  |  | X |  |  |
| Actions which could compromise the staff member’s professional standing | | X | X |  |  |  | X |  |  |
| Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy | | X | X |  |  |  | X |  |  |
| Using proxy sites or other means to subvert the school’s / academy’s filtering system | | 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 |  |  |
| Breaching copyright or licensing regulations | | X | X |  |  |  | X |  |  |
| Continued infringements of the above, following previous warnings or sanctions | | X | X |  |  |  | X |  |  |

22

# Pupil Acceptable Use Policy Agreement

#### 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 / tablets
* 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 / tablet
* I understand that no device suitable for internet connection is allowed in the school or when travelling to or from school.
* I understand that mobile phones are not allowed in school.
* If using a computer out of school I understand that I must use it responsibly so as not to cause harm or offence to anyone.

Signed (child):

Signed (parent):

**DATA COLLECTION FORM Appendix 1**

Please complete the details below and return this form to your child’s teacher as soon as possible

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Surname: |  | Legal Surname:  (if different) | |  | | |
| Forename: |  | Middle Name: | |  | | |
| Chosen Name: |  | Gender: | M / F | | Class |  |
| Date of Birth: |  | Brother/Sister in school | | | | Yes / No |
| Address:  (Must include house number) |  | | | | | |
| Postcode: | | | | | |

Please give details of all persons who have parental responsibility and anyone else you wish to be contacted in an emergency. Place them in the order that you wish for them to be contacted.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Surname: | | Forename: | | | Mr/Mrs/Ms | Relationship | | | | Priority |
| Address: | | | | | | Postcode: | | | | |
| Home Tel: | Work Place: | | | Work Tel: | | Mobile: | | | | |
| Surname: | | Forename: | | | Mr/Mrs/Ms | Relationship | | | | Priority |
| Address: | | | | | | Postcode: | | | | |
| Home Tel: | Work Place: | | | Work Tel: | | Mobile: | | | | |
| Surname: | | Forename: | | | Mr/Mrs/Ms | Relationship | | | | Priority |
| Address: | | | | | | Postcode: | | | | |
| Home Tel: | Work Place: | | | Work Tel: | | Mobile: | | | | |
| Doctor: | | | | | | Telephone: | | | | |
| Address: | | | | | | | | | | |
| Medical Information:  ***It is very important for the school***  ***to be aware of any medical issues*** | | | | | | | | | | |
| Special Dietary Needs: | | | | | | | | | | |
| Home Language:  See overleaf | | | Ethnicity:  See overleaf | | | | Religion:  See overleaf | | | |
| Referred to Educational Psychology Service | | | | | | | | Yes | No | |
| Diagnosed with any specific Learning Difficulties | | | | | | | | Yes | No | |
| Consent for my child/children to travel to school organised events, e.g. trips or sporting occasions | | | | | | | | Yes | No | |
| Consent for my child’s/children’s image to appear in local newspapers, wall displays, school website or videos of school productions | | | | | | | | Yes | No | |
| Consent for my child’s/children image to appear in the school Facebook page or school Twitter account without naming the child | | | | | | | | Yes | No | |
| I wish to receive the school information sheet by email using the address below; | | | | | | | | Yes | No | |
| Signed: | | | | | | | | Date: | | |

Data Protection Act 1998: The school is registered under the Data Protection Act for holding personal data. The school has a duty to protect this information and to keep it up to date. The school is required to share some of the data with the Local Education Authority and with the Department of Education.

The following table outlines the categories used by the Department of Education for the School Census returns.

The categories are listed in Alphabetical order in each column.

Please indicate your selection in the appropriate section on the attached form.

|  |  |  |  |
| --- | --- | --- | --- |
| Home Language | Ethnicity | Religion | |
| Bengali  Cantonese  English  Gujarati  Hindi  Irish  Mandarin  Other  Punjabi  Urdu  Vietnamese  Unclassified | Black – African  Black – Caribbean  Bangladesh  Black – Other  China / Hong Kong  India / Sri Lanka  Korean  Mixed Ethnic Group  Malaysia  Other Non White  Pakistan  Traveller  Vietnam  White | Baptist  Bahai  Brethren  Buddhist  Congregational Church  Church of England  Church of God  Church of Ireland  Church of Scotland  Elim  Free Methodist  Free Presbyterian  Hindu  Independent Methodist  Jewish  Jehovah Witness | Methodist  Church of Jesus Christ of LDS  Muslim  Moravian  No Religion  Other Christian  Other Protestant  Pentecostal  Presbyterian  Quaker  Roman Catholic  Salvation Army  Seventh Day Adventist  Sikh  Unclassified |