PREVENT DUTY

1. Aims: Preventing Radicalisation

Protecting children from the risk of radicalisation should be seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation it is possible to intervene to prevent vulnerable people being radicalised. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The Internet and the use of social media in
particular has become a major factor in the radicalisation of young people. As with managing other safeguarding risks, staff should be alert to changes in children's behaviour, which could indicate that they may be in need of help or protection. School staff should use their professional judgement in identifying children who might be at risk of radicalisation and act proportionately, which may include making a referral to the Channel programme. From 1 July 2015 specified authorities, including all schools (and since 18 September 2015 all colleges) as defined in the summary of this guidance, are subject to a duty under Section 26 Counter-Terrorism and Security Act 2015 ("the CTSA 2015"), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent Duty.

The school staff responsible for the Prevent Duty is the Head Teacher, who is the Prevent Officer.

EYFS key themes and commitments

A Unique Child	Positive Relationships	Enabling Environments	Learning and Development
1.3. Keeping Safe	2.1. Respecting each other 2.2. Parents as partners	3.4. The wider context	4.4. Personal, social and emotional development

PREVENT STATEMENT

PREVENTING RADICALISATION IN SCHOOL

LPEBL is fully committed to safeguarding and promoting the welfare of all its pupils. As a school we recognise that safeguarding against radicalisation is as important as safeguarding against any other vulnerability.

All staff are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs. We believe that children should be given the opportunity to explore diversity and understand Britain as a multi- cultural society; everyone should be treated with respect whatever their race, gender, sexuality, religious belief, special need, or disability.

On 1 July 2015, Section 26 Counter-Terrorism and Security Act 2015 came into force. This duty places the responsibility on local authorities and schools to have due regard to the need to prevent people from being drawn into terrorism. As part of our commitment to safeguarding and child protection we fully support the government's *Prevent Strategy*.

At La Petite Ecole Bilingue we take this duty seriously and carry out the four main actions responsibly, theseare:

- RISK ASSESSMENT**:** assess the potential risk within the school of radicalisation (this action forms part of our child protection policy)
- WORKING in PARTNERSHIP with the local community and local education authority. Being aware of the latest requirements and having a clear line of communication with the local authority Prevent lead.
- PROVIDING APPROPRIATE STAFF TRAINING**.** All staff receive annual safeguarding training and all new staff including volunteers are fully receive a thorough induction process.
- Policies: all our statutory policies are reviewed and available to read from the school website or on request.

WHAT WE DO IF THERE IS A CONCERN

La petite Ecole Bilingue - OG Prevent lead officer: Helene Knupffer

If we have a concern about a particular pupil/family, we will follow the school's normal safeguarding procedures, including discussing with the school's designated safeguarding officer (s), the school's prevent officer and where deemed necessary, with children's socialcare.

2. Monitoring the Use of Online Technology

Use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; and sexual predation. Technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

The LDCPO shall ensure that as part of the requirement for staff to undergo regularly updated safeguarding training (Keeping Children Safe in Education 2018paragraph 75) and the requirement to ensure children are taught about safeguarding, including online (Keeping

Children Safe in Education 2018 paragraph 77), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. As such proprietors and head teachers should ensure appropriate filters and appropriate monitoring systems are in place. Peer on peer abuse can manifest itself in many ways.

Proprietors and head teachers should ensure sexting and the school or colleges approach to it is reflected in the child protection policy.

Other Legal framework:

- Revised Prevent duty guidance for England and Wales (Counter-Terrorism and Security Act 2015)
- Behaviour and Discipline in Schools 2016- departmental guidance for school leaders and school leaders and school staff on developing a school behaviour policy (DPE- 00023-2014)
- Preventing and Tackling Bullying 2017: Advice for school leaders and staff (DPE- 00160-2017)
- Approaches to preventing and tackling bullying: case studies (2018) (DFE- RR751)

E-Safety and Acceptable Use of the Internet Policy

1.Introduction

1.1 Rationale for the need for an e-safety and Acceptable Use of the Internet Policy

This policy represents The Stewart Bilingual School's approach to ensuring that **e-Safety** (electronic safety) is embedded in the use by pupils and staff of devices that can access the Internet. E-Safety at LPEBL:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and the use of new technologies in a positive way;
- focuses on education about the risks as well as the benefits, so that users feel confident online;
- aims to help pupils to develop safer online behaviours both in and out of school; and
- aims to help pupils recognise unsafe situations and know how to respond to risks appropriately.

1.2 What does the policy cover?

E-Safety covers not only Internet technologies but also any electronic communication via smart phones, tablets, laptops, or any wireless enabled technology. When the word "**Internet**" is used in this policy it refers to any online activity e.g. Email, Internet access, cloud storage or interaction with the Virtual Learning Environment (VLE * If applicable).

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The Stewart Bilingual School's e-Safety and Acceptable Use of the Internet Policy must reflect this by keeping abreast of the changes taking place. LPEBL School has a duty of care to enable pupils to use online systems safely. **This policy will be reviewed on an annual basis.**

1.3 Links to other school policies

The e-Safety and Acceptable Use of the Internet Policy operates in conjunction with other school policies including; Safeguarding and Child Protection Policy and Positive Relationships and Anti-Bullying Policy. E-Safety at LPEBL is built into the delivery of the curriculum. As ICT is a compulsory cross-curricular element of the revised curriculum, this policy is intended to ensure the safe acquisition, development and use by pupils of these skills at The Stewart Bilingual School.

1.4 What is the Internet?

The Internet is an electronic information highway connecting computers all over the world and millions of individual subscribers. This global "network of networks" is not governed by any entity. This means that there are **no limits** or checks on the kind of information that is maintained by, and accessible to, the Internet. The educational value of appropriate use of information and resources located on the Internet is substantial, allowing for the efficient digital exchange of appropriate information between pupils, staff and parents.

1.5 What is a VLE?

A Virtual Learning Environment (VLE) is a range of educational resources, comprising information, forums, assessments and other online material provided to students as part of an online learning package. Currently VLE is very rarely used at The Stewart Bilingual Schoo, which is a screen free school.

1.6 Why use the Internet?

The Stewart Bilingual School allows use by pupils of the rich information sources available on the I n t e r n e t . Online resources offer a broader range of up-to-date resources to pupils (both those at school and those unable to attend school), provide an independent research facility, facilitate a variety of learning styles and abilities and encourage pupils to take responsibility for their own learning.

1.7 Networked access to Internet

In recognition of these benefits, The Stewart Bilingual School offers networked Internet, VLE and email access for staff only. Appropriate cross-curricular use of the Internet and the VLE is not actively encouraged as the school prefers to use traditional means of teaching.

1.8 How will pupils gain access to the Internet and VLE at The Stewart Bilingual School?

- In ICT specific lessons.

- Through non ICT subject use across the curriculum.

1.9 Use of pupil owned mobile Internet enabled devices

Under certain conditions (as outlined in section 11) LPEBL School supports pupils using their own personal devices to further their learning, such as Kindle for reading. The opportunities to use the Internet and access online resources are restricted by access to school specific equipment.

In school, pupils are **strictly forbidden** to access Internet resources outside the school network such as those provided through phone 3G/4G contracts.

Pupils are solely responsible for their own devices if being used at school. The school does not accept responsibility for damage or loss to these devices and it is the pupils' responsibility to ensure they are kept secure at all times.
Section 11 of this policy outlines guidelines relating to '**bring your own device'.**

1.10 Dangers in using the Internet

Since the Internet is composed of information from a vast array of sources worldwide, it includes some material that is not of educational value in the context of the school. This material includes information that may be inaccurate, abusive, sexually oriented, racist, sectarian or illegal. In order to guard young people from danger, it is the joint responsibility of school staff and the parent or guardian of each pupil to educate the pupil about her responsibility when using the Internet. The schools' e-Safety and Acceptable Use of the Internet Policy is written in order to address these dangers and promote safe online use.

1.11 Promoting awareness of the e-Safety and Acceptable Use of Internet Policy

The Stewart Bilingual School will endeavour to ensure that all stakeholders are made aware of this policy. The policy will be made available to parents, pupils, governors and staff. A copy will also be available on the website.
The HT, DH and proprietor will oversee eSafety training, policy and procedures.

Policy development

- HT/DH and proprietor management meeting
- Staff consultation.
- School Council.
- Parental consultation.

2.0 Roles and Responsibilities

2.1 Pupils' responsibilities

Pupils are responsible for good behaviour on the Internet just as they are in the classroom, school corridor or school buses, so normal school rules will apply. In addition, a number of rules relating specifically to use of the Internet also apply.

2.2 Pupils' unacceptable behaviours

Misuse of the Internet is a breach of LPEBL School Positive Behaviour and Citizenship policy and will incur the relevant sanctions. The following list applies to all uses of the Internet and mobile technologies including email, social media (Facebook, Instagram, Twitter, Snapchat etc), texting and messaging.

Examples of misuse of the Internet include the following. This list is not exhaustive.

- taking, retrieving, sending, copying or displaying impolite, discourteous or offensive images/text/messages/videos
- causing persistent irritation and/or wilful embarrassment to a member of the school community.
- send or play offensive sound recordings
- cause distress to another member of the school community
- making false allegations against others/written provocation against others.
- making racial, sectarian or homophobic comments
- harass, insult, bully or attack others
- refusing to follow teachers' instructions
- bringing the school into disrepute
- cheating
- damage or tamper with computers, computer systems or computer networks
- copying, saving and/or redistributing copyright protected material
- copy software from or to the school computer systems without prior permission from a teacher
- using the school computer systems to create or distribute malicious materials or software
- using the school computer systems to create or distribute software that could cause a security breach
- use or attempt to use another user's password to access his/her network area
- trespass in another user's folders, work or files
- intentionally waste resources (such as consumables e.g. paper and toner)
- use the network for unapproved commercial purposes
- use ICT resources in any way that contravenes Health and Safety guidelines
- take part in any form of cyberbullying
- subscribe to any services or ordering any goods or services, unless specifically approved by the school
- search or view materials that are not related to the curriculum or future careers
- play computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher
- use the network in such a way that use of the network by other users is disrupted
- publish, share or distribute any personal information about a user
- carry out any activity that violates a school rule
- using or distributing by whatever means any material relating to school activities pupils or staff for which explicit permission has not been given
- engaging in any online activity that is harmful or hurtful to others, and
- taking or receiving pictures, videos, sound clips of pupils for which explicit permission has not been given by a teacher

2.3 Acceptable pupil behaviour

Online activities which are encouraged include, for example:

- use of the Internet to investigate and research school subjects, cross-curricular themes and topics;

- the development of pupils' competence in ICT skills and their general research skills.

2.4 Activities by pupils making reference to school name, staff members or pupils

Pupils should note that using or distributing via online mechanisms (including on social networking sites or similar) any material relating to school activities, pupils or staff for which explicit permission has not been given is unacceptable.
This includes the posting of material, images or video footage relating to school staff, pupils, the school environment or school name. This applies to curricular and extra-curricular aspects of school life as well as to all school trips.

2.5 Action in the event of unacceptable behaviour by a pupil

If a pupil is discovered to be using the Internet in a way that it is deemed to have contravened this Acceptable Use of the Internet Policy, subsequent actions will follow the schools standard disciplinary procedure.

Serious breaches of non-permitted activities or concerns may result in local authority or PSNI involvement.

2.6 Action in the event of a pupil or member of staff being able to access/view inappropriate material online

If at any time a member of the school community finds that she/he is able to access, from within the school, Internet sites which are unsuitable or should be blocked she/he should close the site down and, in the case of a pupil, advise a staff member immediately. The staff member should report the incident as soon as possible to the Principal so that the site can be blocked (if appropriate) and the incident recorded in the Online Safety Register (Appendix 5).

2.7 Location and supervision of Internet based access

Internet access is available for pupils at LPEBL at any networked computer around the school. This access will always be directly supervised (within a class).

3.0 Acceptable use of digital photographs, images or videos of pupils

3.1 Parental consent for the taking of digital photographs or videos of pupils

All parents are issued with a permission request for photographs to be taken and displayed and an image of each child is taken for the computer system in the back to school questionnaire. The details of the parental response are held in the school office. Staff should check these details prior to image use.

Digital photographs or video may be taken at school activities and during the academic year and may be used, with parental consent, for display purposes in the school, for publication in the press or for promotional purposes.

For displays/use outside school or where staff require additional guidance on the display/use of photographs, the Senior Leadership Team should be consulted.

4.0 Training to support e-Safety

4.1 Pupil training

The Stewart Bilingual School will endeavour to ensure that all pupils understand how they are to use the Internet, VLE and email appropriately and why the rules exist.

NPCC and Prevent team resources are a useful teaching tool for all Key Stages looking at Internet safety. Pupil awareness training around Internet e-Safety issues is incorporated into the pupils' ICT programme of study. It is further supported through the schools pastoral programme. Training and support includes:

- specific e-Safety lessons - NPCC training;
- guidance by individual teachers on safe Internet practice;
- reinforcement of e-Safety issues through the assemblies and in classroom.

4.2 External support resources

There are many appropriate resources now available in relation to Internet and e-Safety. These are available freely to parents and pupils. Childnet, as an example, has produced many materials to support the teaching of e-Safety at different key stages. They have also produced materials for parents, staff and post primary pupils. Websites to look at include *www.childnet.com, www.ceop.police.uk/, www.internetmatters.org, www.kidsmart.org.uk/beingsmart, www.thinkuknow.co.uk*

5.0 Risk assessments

LPEBL School will perform risk assessments on the technologies within the school to ensure that it is aware of and, mitigates against, the potential risks involved with their use.

5.1 Risk assessment process

- particular care should also be taken when accessing the sites while projecting the computer desktop on a whiteboard, as inappropriate material may be openly displayed.

6.0 Cyber bullying

The Stewart Bilingual School takes cyber bullying very seriously. This form of bullying is considered within its anti- bullying policy and pastoral programme as well as within this policy.

Teachers are to be aware that social media sites can offer much with regards to teaching and learning experiences for the pupils, but that they bring their own unique issues and

concerns.

Each social media technology that is to be utilised, should be risk assessed by teachers in the context of each school situation. Risk assessment form (appendix 4) should be completed before the use of a social media site is authorized in a classroom context.

6.1 Forms that cyber bullying can take.

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Using any form of technology to blackmail or extort.

6.2 What to do if pupils feel they are being cyber bullied

Pupils are encouraged to report incidents of cyber-bullying to both the school and their parents to ensure the matter is properly addressed and the behaviour ceases.

The Stewart Bilingual School records all instances of cyber-bullying incidents to monitor the effectiveness of their preventive activities, and to review and ensure consistency in their investigations, support and sanctions.

- **See also:** Cyberbullying: advice for headteachers and school staff (DPE- 00652- 2014)

7.0 Email and Internet security

7.1 Email Security

Staff are advised to only use the school email system. At LPEBL any communication between parents and staff is done via communication book first.

10.0 Information for Parents and pupil consent forms

Parents are informed in writing of the schools e-Safety and Acceptable Use of the Internet Policy. They are asked to give permission for their children to use the Internet. Pupils are also required to sign an undertaking agreeing to their proper use of the Internet.

10.1 Guidance for parents with Internet access at home

It is strongly advised that a home computer/mobile device with Internet access should be situated in a location where parents can monitor access to the Internet. Computers should be fitted with suitable anti-virus, antispyware and filtering software.

Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use.

Parents should become familiar with the sites their children visit, and talk to them about

what they are learning. Parents should use appropriate Internet filtering software for

blocking access to inappropriate materials.

Parents should consider carefully whether children should have access to social networking sites e.g. facebook and what restrictions are needed to ensure safe use of such sites.

Parents should ensure that they give their agreement before their children give out personal information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images.

Further free advice for parents is available from the following sources:

www.thinkuknow.co.uk
www.kidsmart.org.uk
www.getnetwise.org

11.0 Pupils bringing their own device to school

11.1 Request and Instruction

During the school day the use of devices owned personally by pupils is subject to the same requirements as technology provided by the school. LPEBL School recognises the opportunities that exist for pupils to actively learn through using their own device at school. It supports their use within the learning context with the understanding that controls must be put in place for their safe use.

The rules governing pupils using their own devices are either by **REQUEST** from the pupil or **INSTRUCTION** from the teacher.

REQUEST

In this situation, the pupil makes a request that she use her own device to access the Internet or use the device to further her learning in the classroom or at school. The teacher responds to this request by the pupil for the duration of that lesson only.

INSTRUCTION

The teacher gives instruction as appropriate for pupils to use their own device.

11.2 Conditions for pupils using their own devices

1. The device must be used in accordance with the e-Safety and Acceptable Use of the Internet Policy.
2. Any inappropriate content stored on the device in breach of the e-Safety and Acceptable Use Policy must be removed before it is brought into the school premises.
3. Pupils should have an up-to-date anti-virus/Internet security product on their device.
4. Acceptance that the school **takes no responsibility** for any device brought into school.
5. Parents/Guardians should have appropriate insurance measures in place to cover the device for this application.
6. The pupil is solely responsible for the safety (including content) of the device on his/her way to school, during school and on the return from school.
7. Use of the Internet and email is monitored and, any use deemed to be inappropriate, will be dealt with using the school's disciplinary procedures and policies.
8. If a teacher suspects school rules have been broken, pupils can be asked to display images stored on their device.
9. If inappropriate and/or illegal materials are discovered, then the incident will be pursued through the schools' disciplinary procedure.
10. There should be no use of cameras (if available on the device) to take images or video of pupils or a staff member without explicit staff and pupil permission.
11. Pupils who wish to connect their personal equipment to the school wireless network, should have no expectations of hardware or software support from the school.
12. Devices should be named ideally with a UV pen in accordance with advice from the police.
13. Pupils will be responsible for the security of their passwords and if their device is left unattended, the pupil should have either logged off or locked the device to prevent anyone using it in their absence.
14. If a pupil suspects that her device has been affected by a virus or other malware, it should be removed from the school network and fixed before using on the school network again.
15. Any charging device brought to school must be available for PAT testing to ensure electrical safe

compliance.

Pupils and parents should also note:

- Pupils should be conscious of personal safety when carrying devices to, around and from school.
- Pupils should be conscious of personal safety when communicating online, and therefore will not share unnecessary personal information about themselves or others.
- It is also the user's responsibility to ensure that, where possible, devices brought in to school have an up-to-date anti-virus/Internet security program that receives regular updates. Failure to do so may result in viruses being transferred to school computers via email, removable storage devices or by access to the school folders remotely.

11.3 Agreement to guidelines "bring your own device"

To enable pupils to use their own device at school, under the terms of the e-Safety and Acceptable Use of the Internet Policy, written permission is required. Parents/guardians should sign and return the permission form for pupil Internet access and bring your own device.

Appendix 2

Dear Parent/Guardian,

e-Safety and Acceptable Use of the Internet Policy – Permission form

As part of the school's ICT strategy, LPEBL School offers pupils access to a filtered Internet service. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on Internet access and use.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any

disadvantages. We have put in place a filtered Internet and e-mail service to minimise the dangers of pupils gaining access to unsuitable materials. In addition, a clear set of rules and procedures for pupil use of the Internet has been implemented. Ultimately, however, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources.

During class, teachers will guide pupils towards appropriate materials. Clear rules and procedures are in place for proper use of the Internet. Outside of school, families must bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Appropriate home use of the Internet by children can be educationally beneficial and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home.

Whilst we endeavour to continue to educate in this challenging area, pupils are only permitted to access online materials using Internet connections provided and filtered by, or on behalf of, The Stewart Bilingual School. We appreciate your ongoing support as we work together to ensure the safety of your child and those in our wider school community.

Free eSafety advice is widely available on the Internet, examples include: from the following sources: http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms. http://www.parentsonline.gov.uk/ - promotes home school links by helping parents understand the role of ICT in learning http://www.getnetwise.org/ - information about filtering programs for home use
We would be grateful if you could read the enclosed guidance documents and then complete the

permission form which follows. Yours sincerely

LPEBL School Pupil Internet Access and 'Bring Your Own Device' Consent Form

Please complete and return this form to enable your daughter to access the Internet at school. The form also authorizes your daughter to bring her own device to school and for her to use the device within the terms as outlined in the e-Safety and Acceptable Use of Internet Policy.

By signing this form you:

1. Have read and understood the e-Safety and Acceptable Use of the Internet Policy and agree to abide by this policy
2. Confirm that a device brought to school by your daughter will **only be used in** accordance with this policy
3. Confirm that you accept full responsibility for the full replacement value of all electronic equipment which the pupil mentioned below brings into school.
4. Understand that the school's Internet services are filtered in an effort to prevent pupils from coming into contact with objectionable material; however incidents may still occur when inappropriate material has not been blocked by the filtering service.
5. Understand that your daughter must comply with The Stewart Bilingual School's e-Safety and Acceptable Use of the Internet Policy and support the sanctions that are outlined in the schools disciplinary policy.

This contract will remain in force **throughout the pupil's time** at school and may be revised to take account of technological advancements in the interests of pupil safety. Return the signed form to the school office/form teacher.

As the parent or legal guardian of the pupil below, I **grant permission** for my daughter to use the Internet and bring her own device to school.

Parent's/Guardian's Agreement

NAME of Pupil: _____(Please Print)

Signed Parent/Guardian: _____ Date: _____

Pupil's Agreement

I have read and understand the Pupils' Roles and Responsibilities (Section 2.0) & Guidance for Pupils on the use of the Internet (Appendix 3). I will use the computer system, including my own devices, in a responsible way and obey the school rules at all times.

Signed Pupil: _____ Date: _____

The information on this form is covered by the provisions of the Data Protection Act, 2018. Your signature on the form is deemed to be an authorization by you to allow the School to process and retain the information for the purpose(s) stated

Guidance for pupils on the use of the Internet

The Stewart Bilingual School encourages use by pupils of the rich information sources available on the Internet and t h e schools virtual learning environment (Fronter). Online resources offer a broader range of up-to-date resources to pupils; provide an independent research facility; facilitate a variety of learning styles and abilities and encourage pupils to take responsibility for their own learning.

Access to the Internet, email and online resources is a privilege, not a right and this facility must be used responsibly. Parental consent and permission is required. All individual users are responsible for their behaviour and communications over the network. It is presumed that pupils will comply will school standards and the agreements they have signed.

Guidelines for pupils:

- Passwords are private and should **not** be given out under any circumstance
- **Do not publish** in any form another pupils **personal details** (including images) via Fronter/Internet or email
- **Any files** downloaded/uploaded **should not** offend or **be inappropriate** in any way
- Help protect yourself by **informing teachers** of any **inappropriate communications** you receive whilst online or using the Internet
- **Do not damage** or interfere in any way with the schools fixed or mobile computer equipment. This includes **not drinking/eating** whilst using the school's computer equipment
- **Any damage** discovered to the school's computer equipment should be **notified to a teacher** or a member of school staff
- Do not attempt to **open/copy/change** or delete **another pupil's files**

The following are **NOT** permitted and are **UNACCEPTABLE**:

- retrieve, send, copy or display offensive messages or pictures;
- send or play offensive sound recordings;
- use obscene or racist language;
- harass, insult, bully or attack others;
- damage or tamper with computers, computer systems or computer networks;
- violate copyright laws;
- copy software from the school computer systems;
- copy computer software, including computer games on to the school systems;
- give out their C2K password to anyone;
- use or attempt to use another user's password to access his/her network area;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as consumables e.g. paper and toner);
- use the network for unapproved commercial purposes;
- use ICT resources in any way that contravenes Health and Safety guidelines;
- use anydevice to access the Internet unless access is through the C2K managed system;
- any form of cyberbullying.

For information about personal safety when online please refer to

- www.thinkuknow.co.uk
- www.childnet.com
- www.kidsmart.org.uk