# THE HARVEY GRAMMAR SCHOOL


Founded 1674

# e-SAFETY POLICY

**Adopted October 2016**

## 1. INTRODUCTION

In today's society, children, young people and adults interact with technologies such as mobile phones, tablets, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

"e-Safety" or online safety covers issues relating to children and young people as well as adults, and their safe use of the Internet, mobile phones, tablets and other electronic communications technologies, both in and out of school or settings. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. It should be noted that the use of the term 'online safety' rather than 'e-Safety' should be used to reflect the wide range of issues associated with technology and a user's access to content, contact with others and behavioural issues and is a move away from being regarded as an ICT issue.

The Policy has been devised in consultation with staff, pupils, parents and governors and will operate in conjunction with other school policies, including those for Behaviour and Anti-Bullying, and will be reviewed, along with its implementation, bi-annually.

### 1.1 Aims and policy scope

The Harvey Grammar School has a duty to provide quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions. The Harvey Grammar School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of The Harvey Grammar School's online safety policy is to:

- Clearly identify the key principles expected of all members of the school with regards to the safe and responsible use technology to ensure that the school is a safe and secure environment.
- Safeguard and protect all members of the school online.
- Raise awareness with all members of the school regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops tablets or mobile phones. This policy must be read in conjunction with other relevant school policies

## 2. INTERNET ACCESS

Internet use is part of the statutory curriculum and is a necessary and important tool for learning and an essential element of everyday life for education, business and social interaction. The school therefore has a duty to provide its pupils with quality Internet access as part of their learning experience to enable them to learn how to evaluate Internet information and to know how take care of their own safety and security when using the Internet outside school.

Used wisely, the Internet can help the school to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the effectiveness and efficiency of the school's management functions.

## 2.1 Educational benefits of Internet use

It is widely accepted that the benefits of using the Internet in education include:

- Providing pupils and staff with access to world-wide educational resources including museums and art galleries
- Making the school part of the National Education Network which connects all UK schools
- Enabling educational and cultural exchanges between pupils world-wide
- Providing vocational, social and leisure use in libraries, clubs and at home
- Enabling access to experts in many fields for pupils and staff
- Encouraging professional development for staff through access to national developments, educational materials and effective curriculum practice
- Fostering collaboration across networks of schools, support services and professional associations
- Improving access to technical support including remote management of networks and automatic system updates
- Facilitating exchange of curriculum and administration data with the local authority and the Department for Education
- Giving access to learning wherever and whenever convenient

## 2.2 Use of the Internet to enhance learning

The school spends a significant amount each year on ensuring there are sufficient computers available for staff and pupils to use, each with high-speed Internet access, and so must consider the impact on pupils' learning outcomes. Developing effective practice in using the Internet for teaching and learning is essential if pupils are to learn high-level digital literacy skills which they will need in order to refine their own publishing and communications with others via the Internet. This will require pupils to have appropriate respect for copyright, intellectual property rights and the correct use of published material, while the school will develop effective strategies to detect and deal with plagiarism.

Policy statements:

- The school's Internet access will be designed to enhance and extend learning opportunities
- Pupils will be taught to distinguish between acceptable and unacceptable on-line activities and will be given clear objectives for Internet use, including the effective use of the Internet in research and the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law

## 2.3 Evaluating Internet content

Twenty-first century citizens need to develop critical skills in how to select and evaluate the quality of information received via the media, including the Internet. Dealing with information gained on-line requires particularly well-developed digital literacy skills as it is often difficult to determine its origin, intent or accuracy as the contextual clues may be missing or difficult to read.

Policy statements:

- School Internet access will be designed expressly for student use and will include filtering appropriate to the age of the students
- Pupils will be taught to be critically aware of the materials they read on-line and will be shown how to validate information before accepting its accuracy

## 2.4 Security of information Systems

The school has a major responsibility to ensure not only the delivery of essential learning services but also the personal safety of staff and pupils. ICT security is a fundamental aspect of the safeguarding requirements with which the school must comply and everyone in the organisation has his/her part to play in this respect.

All school computers are part of both a Local Area Network (LAN) - which now extends to include individuals own personal devices via wireless – and a Wide Area Network (WAN) via the Kent Public Service Network (KPSN) broadband connection.

Policy statements:

- The school will expect all users to act reasonably (e.g. refrain from playing internet-based games as this adversely affects the service that others receive) and take responsibility for their network use
- Pupils who fail to act responsibly will be disciplined according to the sanctions given in the school's Behaviour Policy. For staff, flouting electronic use policy will be regarded as a serious disciplinary matter and possible reason for dismissal
- All workstations will have continuously updated anti-virus protection
- All servers will be kept in a secure location with restricted physical access restricted and server operating systems will be kept up to date and secured with regularly updated anti-virus protection
- Access to the network by wireless devices will be carefully controlled by the network management team
- All Internet connections will be via the KPSN Schools Broadband network to prevent unauthorised access between schools and which is monitored and maintained by a specialist security command centre
- The security of the school information systems and users will be reviewed regularly
- Offsite access to the network will be via a secure connection
- Only software approved and installed by the network management team may be used on the network. The network management team will regularly check users' files and e-mail accounts to ensure compliance

## 2.5 Email

Email is an essential means of communication for both staff and pupils but brings with it certain security and safeguarding implications. In the school context (as in the business world), email should not be considered private and the school reserves the right to monitor email to maintain the safety of pupils while at the same time respecting their human rights. Spam, phishing and virus attachments can make email dangerous and KPSN uses industry leading email relays to stop unsuitable mail arriving in schools (currently about 95% of mail is rejected as spurious).

Policy statements:

- Pupils should use only their school email accounts when communicating to and from school
- Pupils must immediately report to a member of staff if they receive email which is offensive or has a suspicious attachment
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from their parent/carer

- Pupils and staff should ensure that email sent to external organisations from school email accounts does not reflect badly on the school in any way – such communication is equivalent to a letter written on school headed paper
- The forwarding of chain messages is not permitted
- Staff should use only school email accounts when communicating with pupils

### 2.6 Publishing pupil's images, work or videos online

Publishing still and moving images on the school's website can give a real flavour of the school in action but care must be taken not to compromise the security of staff and pupils. Displaying individual pupils' names with their images is not acceptable as such images could be re-used for inappropriate purposes. In accordance with the "use of photographic images of children" advice on the Children's Safeguards site at www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety, the school's policy statements are therefore:

Policy statements:

- Images on the school website which include pupils will be selected carefully and will not provide material that could be reused
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images of pupils are electronically published
- Pupils will be taught the reasons for caution in publishing personal information and images online
- Personal information on staff or pupils will not be published on the school website
- The Headteacher has overall editorial responsibility for the school website and the Intranet and will ensure that published content is accurate and appropriate and complies with the school's guidelines for publications, including respect for intellectual property rights and copyright

### 2.7 Online spaces and social networking

It is crucial that parents/carers and teachers are aware of the rapid evolution of online spaces and social networks which allow individuals to publish unmediated content. Social networking sites such as Facebook can connect people with similar or even very different interests and invite users to view personal spaces and leave comments, over which there may be limited control.

Pupils need to be educated so that they realise the dangers in uploading personal information – the ease with which such sites can harvest confidential data and the difficulty of removing an inappropriate image or information after it has been submitted.

All staff should be aware of the potential risks to them of using social networking sites, particularly when sharing personal information with other users of the sites who may be pupils at the school. They should also be aware of the importance of considering the material they post, ensuring their profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of such sites include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Policy statements:

- Expectations regarding safe and responsible use of social media will apply to all members of The Harvey Grammar School and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin

boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others

- All members of The Harvey Grammar School are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any public social network space and to avoid including background detail in a photograph which could identify them or their location
- Pupils will be encouraged to invite known friends only (which should not include members of staff) and deny access to others by making profiles private
- Staff will not include pupils within their group of friends on social network spaces
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications

## 2.8 Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF 2007). Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life but, unfortunately, such technologies can also be used negatively. Anyone – children or adult – can be the target of bullying via mobile phones, on-line games or the internet, and a once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that all pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. The government and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

Policy Statements:

- The school will not tolerate cyberbullying (along with any other form of bullying) – see the school's Anti-Bullying Policy
- The school will have clear procedures in place to support anyone affected by cyberbullying and all incidents of cyberbullying reported to the school will be recorded and dealt with according to the school's Anti-Bullying Policy
- The school will involve the police and/or the Children's Safeguarding Unit in incidents of cyberbullying where appropriate

## 2.9 Filtering

Levels of Internet access and supervision will vary according to the pupil's age and experience. Older pupils, as part of a supervised project, might need to access specific adult materials - for instance a course text or set novel might include references to sexuality- while teachers may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, the restrictions imposed by the school's filtering system may be removed temporarily while the user accesses the material under close supervision.

Policy statements:

- The school will work with our internet provider to ensure that systems to protect users are constantly under review

- The school will apply the KCC-recommended filtering system to all Internet access
- Staff and pupils who discover that an unsuitable site is accessible must report this to the school's e–Safety Coordinator
- The e-Safety Coordinator will manage the configuration of the filtering system to ensure that it is appropriate, effective and reasonable
- The school will report any on-line material it believes to be illegal to the appropriate agencies such as IWF or CEOP

## 2.10 Videoconferencing

Videoconferencing enables users to see and hear each other between different locations and this 'real time' interactive technology has many potential benefits to schools. The equipment involved ranges from a web camera attached to a single computer to large room-based systems that can be used for whole classes or lectures.

The school can access the National Educational Network (NEN), a private broadband, IP network interconnecting the ten regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks, via the KPSN.

Policy statements:

- Any videoconferencing equipment in classrooms will be switched off when not in use and not set to auto answer
- Pupils will not take part in a videoconference call without permission from their parents/carers and the supervising teacher
- Videoconferencing will be supervised appropriately according to the pupils' age

## 2.11 Learning Platforms

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across schools; share resources and tools for a range of topics; create and manage digital content; and help pupils to develop secure online e-portfolios.

Policy statements:

- The Senior Leadership Team and network management staff will monitor the usage of the learning platform by pupils and staff
- The school will advise pupils and staff on acceptable conduct and activities when using the learning platform
- Only current members of the pupil, parent/carers and staff community will have access to the learning platform
- All users will be mindful of copyright issues and will only upload appropriate content onto the learning platform
- The school will disable access to the learning platform when staff and pupils leave the school

## 2.12 Emerging technologies

The rapid development of communications technologies offers the school the opportunity to develop new teaching and learning methods as well as enhancing communication between home and school. However,

new technology also brings with it new risks and it is important that clear guidelines are applied and effective and safe practices employed.

Policy statements:

- The school will keep up to date with new technologies and where appropriate conduct risk assessments in order to develop appropriate strategies for their use
- Staff should use a school phone where contact with pupils is required
- Pupils wishing to bring in a mobile device to school must register its details with the School Office and, if it is to be used to access the Internet via the school wireless connection, with the Business Systems Manager
- Pupils may not use mobile phones and hand-held devices in lessons unless the teacher has given permission for them to be used as part of the lesson e.g. researching via the Internet
- Pupils will not use a mobile device to take still or moving images of their peers or members of staff at school or on the way to and from school
- Pupils who send abusive or inappropriate text, picture or video messages will be dealt with under the school's behaviour and/or anti-bullying policies
- Pupils and staff will not upload school-based or school-related material onto an external website which reflects badly on the school

### 2.13 Protection of personal data

The quantity and variety of data held by schools on pupils, families and staff has expanded dramatically over the past few years. While this data is very useful in improving services, it does bring with it the increased need to ensure that it is not mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It applies to anyone who handles or has access to information concerning individuals.

Policy statements:

- The school will record, process, transfer and make available the personal data it holds according to the Data Protection Act 1998

## 3. POLICY DECISIONS

### 3.1 Authorisation of Internet access

Policy statements:

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource
- All pupils must agree to comply with the e–Safety Policy
- All parents/carers will sign and return a consent form regarding pupil access to the Internet

### 3.2 Risk assessment

Policy statements:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The School cannot accept liability for the material accessed, or any consequences resulting from Internet use
- The school will audit ICT use to establish if the e–Safety policy is adequate and that its implementation is appropriate
- The school will make all users aware that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

### 3.3 e–Safety complaints

Policy statements:

- Complaints relating to e-Safety will be dealt with under the School's Complaints Procedure
- Any complaint about staff misuse must be referred to the Headteacher
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken
- The school will liaise with the local Police Safer Schools Partnership Coordinators and the Children's Safeguards Unit when dealing with potentially illegal issues
- The school will deal with any issues (including sanctions) according to the school's disciplinary and child protection procedures

## 4. COMMUNICATION

### 4.1 With pupils

Policy statements:

- The school will ensure that all users are aware that network and Internet use will be monitored
- The school will provide pupils with an e–Safety training module, covering both school and home use, within the ICT programme of study to raise awareness and stress the importance of safe and responsible internet use before pupils are allowed Internet access
- Each subject area will reinforce the importance of safe and responsible use of the internet and new technologies

### 4.2 With staff

It is important that all staff feel confident to use new technologies in teaching and the school e–Safety Policy will only be effective if all staff subscribe to its values and methods.

Policy statements:

- The school will provide the opportunity for all members of staff to contribute to the development and ongoing review of the e–Safety Policy
- The school will ensure that all staff are aware that Internet traffic can be monitored and traced to the individual user and will expect staff to apply high levels of discretion and professional conduct
- The school's Senior Leadership Team will ensure that network management staff who administer filtering systems or monitor ICT are appropriately trained and supervised and be provided with clear procedures for reporting issues
- The school will provide regular updates for staff in safe and responsible Internet use, both professionally and personally

### 4.3 With parents/carers

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

Policy statements:

- The school will provide the opportunity for all parents/carers to contribute to the development and ongoing review of the e–Safety Policy
- The school will ensure that the latest version of the e–Safety Policy is available to parents/carers via the school website and will provide regular information and guidance for parents on e–Safety
- The school will offer e-Safety training to parents/carers with demonstrations and suggestions for safe home Internet use
- Parents will be required to sign an e–Safety/internet agreement as part of the Home-School Agreement

## 5. RESPONDING to ONLINE INCIDENTS and SAFEGUARDING CONCERNS

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. Online Safety (e-Safety) risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Potential concerns can often be dealt with at a personal level by ensuring children are able to identify and speak with a trusted adult. It is important that all children know how to respond if they encounter unsuitable material online.

Teachers and other members of staff are the first line of defence; their observation of classroom behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported and staff will be encouraged to develop a safe culture. Incidents will vary from unintentional jokes or comments, unconsidered inappropriate action to deliberate illegal activity.

The Harvey Grammar School's Designated Safeguarding Leads (DSLs) is familiar with the relevant Kent Safeguarding Children Board Threshold and procedures regarding online safety, including but not limited to:

2.2.2: Children Who Exhibit Harmful Behaviour including Sexual Harm (Assessing and Providing Interventions)

2.2.7: Working with Sexually Active Young People

2.2.9: Bullying

2.2.10: Online Safety, Child Abuse and Technology

2.2.11: Safeguarding Children Abused through Sexual Exploitation

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, The Harvey Grammar School will determine the level of response necessary for the offence disclosed. The decision to involve Police will be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with.

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online safety (e-Safety) incidents may have an impact on pupils, members of staff and the wider school community (both on and off site) and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues will be referred to the school Designated Safeguarding Lead (DSL). Advice on dealing with illegal use internet or technology will be discussed with the Kent Police or the LA Education Safeguarding Team. Incidents and concerns will also be dealt with in line with Kent Police's Schools Policy. hwww.kent.police.uk/about_us/policies/crime-intelligence/n17.html

In some cases the school may feel that it is necessary to contact parents/carers about an issue or alert other local schools. The Harvey Grammar School will ensure that is mindful about the level of information being shared, especially if there is a live police investigation. Sharing specific information which could potentially identify children, families and schools involved or alert offenders to law enforcement investigation could result in children being placed at risk of harm and may prevent appropriate criminal action from being taken. Ultimately this may result in a significant and long term impact on children, families and schools. The school will not release any details regarding on or offline safeguarding concerns (even if they have been shared with from a known or trusted source) which could be of detriment to any children, families or schools involved or that could jeopardise a police investigation. If the school has concerns about on or offline safeguarding issues which we feel need to be shared with parents urgently, or with other schools and settings we will seek advice and guidance from the LA Education Safeguarding Team

Policy statements:

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures
- Complaints about Internet misuse will be dealt with under the School's complaints procedure
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Headteacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate
- The school will inform parents/carers of any incidents of concerns as and when required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the LA Education Safeguarding Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the LA Education Safeguarding Team to communicate to other schools in Kent.

## 6. E–SAFETY CONTACTS AND REFERENCES

| | |
|---|---|
| CEOP (Child Exploitation and Online Protection Centre) | www.ceop.gov.uk |
| **Rebecca Avery**<br>Education Safeguarding Adviser – Online Protection | **Office**: 03000 415797<br>Mobile:07789 968705<br>rebecca.avery@kent.gov.uk **or**<br>for general enquiries: esafetyofficer@kent.gov.uk |
| **Ashley Assiter**<br>e-Safety Development Officer | **Office:** 03000 422148<br>Mobile: 07545 743310<br>ashley.gorton@kent.gov.uk or<br>for general enquiries: esafetyofficer@kent.gov.uk |
| Kent Educational Safeguarding Team | http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding |
| Childline | www.childline.org.uk |
| Childnet | www.childnet.com |
| Children's Officer for Training & Development, Child Protection<br>Mike O'Connell | email: mike.oconnell@kent.gov.uk<br>Tel: 01622 696677 |
| Children's Safeguards Service | www.kenttrustweb.org.uk/safeguards |
| Click Clever Click Safe Campaign | http://clickcleverclicksafe.direct.gov.uk |
| Cybermentors | www.cybermentors.org.uk |
| Digizen | www.digizen.org.uk |
| EIS<br>ICT Support for Schools and ICT Security Advice | www.eiskent.co.uk?ictsecurity |

| | |
|---|---|
| Internet Watch Foundation | www.iwf.org.uk |
| Kent e–Safety in Schools Guidance | www.kenttrustweb.org.uk/esafety |
| Kent Public Service Network (KPSN) | www.kpsn.net |
| Kent Safeguarding Children Board (KSCB) | www.kscb.org.uk |
| Kidsmart | www.kidsmart.org.uk |
| Schools Broadband Team Help with filtering and network security | www.eiskent.co.uk<br>Tel: 01622 206040 |
| Schools e–Safety Blog | www.kenttrustweb.org.uk/esafetyblog |
| Teach Today | http://en.teachtoday.eu |
| Think U Know website | www.thinkuknow.co.uk |
| Virtual Global Taskforce — Report Abuse | www.virtualglobaltaskforce.com |

## 7. DATA PROTECTION ACT 1998

Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Data Protection Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

The Harvey Grammar School will adhere to these principles.