E-Safety Policy

This E-Safety policy has been developed by the Downside School E-Safety Committee which, at the time of creation, comprises of:

- E-Safety Officer
- DSL
- Deputy Head
- Teacher Representative
- Network Manager
- Pupil Representative

Consultation with the whole school community will take place through the following:

- Staff Meetings / INSET Days.
- School Pupil Council
- Appointed School ICT Council
- School Website / Newsletters to Parents.

Schedule for Development, Monitoring and Review:

This E-Safety policy was approved by the E Safety Committee on:	28.3.17
The implementation of this E-Safety policy will be monitored and reviewed by the:	E-Safety Committee
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.	Annually during Term 3

Scope of the Policy:

This policy applies to all members of the Downside School community (including staff, pupils, volunteers, parents/carers, visitors,) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems.

The Education Act 2011 empowers the Head Master, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school.

Roles and Responsibilities:
The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

Governors:
The Governing Body is responsible for the approval of the E Safety Policy and for reviewing the effectiveness of the policy. The review will be undertaken by the Governor's Education Committee (GEC).

Head Master and SLT:
- The Head Master is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Officer.
- The Deputy Head Master is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- The Head Master and members of the SLT will receive a termly report from the E Safety Officer prior to the GEC meeting.
- The Head Master and members of the SLT are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff or pupil. (Appendix 2 of the Child Protection Policy p.32 ff)

E-Safety Officer:
- Chairs the E-Safety Committee.
- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.
- Receives reports of E Safety incidents and creates a log of incidents to inform future E Safety developments.
- Reports termly to the Senior Leadership Team.
- Liaises with Downside School Network Manager.

Network Manager:
The Network Manager takes every precaution for ensuring:
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That he keeps up to date with E-Safety technical information in order to carry out effectively his E-Safety role and to inform and update others as relevant.
- That the use of the network, email are appropriately monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer for investigation / action / sanction.

Teaching and Support Staff:
These users 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 via training and Inset sessions.
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the E-Safety Officer for investigation / action / sanction.
- Digital communications with pupils will always be undertaken on a professional level and in accordance with the Downside School Staff Code of Conduct.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school Acceptable Use Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

- In lessons where Internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are followed for dealing with any unsuitable material that is found in searches.
- At all times, they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- They 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.

Designated Safeguarding Lead (DSL):
The DSL is trained in E-Safety issues and is aware of the potential for serious child protection issues which can arise from the use of the internet and ICT. He will act in accordance with the procedures described in the Child Protection Policy and the South West Child Protection Procedures should any issue arise, particularly in relation to:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- The Prevent Duty

E-Safety Committee:
Members of the E-Safety Committee will assist the E-Safety Officer with the production, review and monitoring of the school E-Safety policy and associated documents.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Are advised with regard to Downside School policies on the use of mobile phones, digital cameras and hand held devices. They are also advised with regard to Downside School 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 and Carers, as Primary Educators, play a crucial part in keeping their children safe and are responsible for:

- Encouraging their child / children follow the Pupil Acceptable Use Policy at home.
- Encouraged to discuss E-Safety issues with their child / children and monitoring their home use of ICT systems (including mobile phones and games devices) and the Internet.

Policy Statements:

Education – Pupils:
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of our 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 education will be provided in the following ways:

- A planned E-Safety programme is provided as part of ICT / Spiritual, Moral, Social and Cultural (SMSC) and other relevant lessons and is regularly revisited. This is outlined in our scheme of work which covers each year group. This ensures that pupils are taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information. It also covers both the use of ICT and new technologies in school and outside school.
- Pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for use of ICT systems / Internet are posted in all ICT rooms and displayed on log-on screens.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Education – Parents / Carers:

Parents and carers will have varying degrees of understanding of E-Safety risks and issues, and in some cases their understanding may be only limited, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents may either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The School therefore seeks to provide information and awareness to parents/carers through:

- An annual parent seminar
- Information sent in the Head Master's Newsletter
- Information sent by the E-Safety Officer

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people named in the Roles and Responsibilities sections are effective in carrying out their E-Safety responsibilities:

- School Servers are securely located and physical access is restricted.
- All users are provided with a username and password by the Network Manager who keeps an up to date record of users and their usernames. Users are required to change their password on a regular basis.
- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Actual / potential E-Safety incidents are reported immediately to the E-Safety Officer who will arrange for these to be dealt with immediately in communication with the Network Manager/DSL, reporting to the Head Master.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Advice is given to staff and pupils about ensuring they have password protection on mobile devices.

Curriculum:

- Where pupils are allowed to search the Internet, eg using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific appropriate search terms to reduce the likelihood of coning across unsuitable material.
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

Use of Digital and Video Images - Photographic, Video (To Correspond with Digital Images Policy)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet.

However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet.

Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. They are advised that they should not store pictures of pupils on school or personal devices but should copy them on to the School's network for storage and then delete them from their personal device.
- Care should be taken when taking digital / video images that pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

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.

N.B. Staff must have regard to the section on roles and responsibilities in which it states that they must:

- Acknowledge by signature their acceptance of the Downside School Acceptable Use Policy.
- At all times, they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- They 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.

They use encrypted memory sticks

Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening, extreme or bullying in nature and must not respond to any such email. They should not delete it.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. It should be only via school approved systems.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Responding to Incidents of Misuse:

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

If any apparent or actual misuse appears to involve illegal activity, such as:

- Indecent images of children.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Radicalisation

Responding to use of a VPN:

Using a Virtual Private Network (VPN) within the school is seen as a deliberate attempt to circumvent the safeguarding filters put in place. As such, a pupil is exposing themselves to inappropriate content including (but not limited to) radical material, pornography and grooming. As such, sanctions apply for using a VPN which are:

First Offence:
The HsM will interview and advise the pupil, and parents will be informed and a written record kept. The pupil will be gated for one weekend, with a two-hour Saturday evening detention during which time the pupil will do some work on VPN awareness or receive a similar punishment.

Second Offence:
Again, the Director of Pastoral will interview and advise the pupil, and parents will be informed in writing by the Director of Pastoral Care. The pupil will be gated for two weekends, with two-hour Saturday evening detentions during which time the pupil will do some work on VPN awareness, or receive a similar punishment.

Third Offence:
The Director of Pastoral Care will interview and advise the pupil, and parents will be informed. The pupil will be referred to the Deputy Head Master and will be suspended from School for three days. The Deputy Head Master will write to the pupil's parents detailing the incident and subsequent action. On return to School, the pupil will be required to see the Head Master, and will be given ongoing advice from the ESafety Officer. In the unlikely event of further offences, the pupil will be suspended from School by the Deputy Head Master for an appropriate time. The Head Master will determine, after a letter of final warning, whether any exclusion will be permanent, and the pupil expelled or required to leave.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. However, if any illegal misuse is

detected or reported action will be taken in accordance with the guidance contained in the section entitled' Procedures for dealing with Inappropriate/Illegal Internet Access or Material' in the Child Protection Policy

(Appendix 2 – Safeguarding and ICT)
click here

Written by:	**Head of Computing and E-Safety Officer**	**11.10.18**
Reviewed & Authorised by:	**Deputy Head Master**	
Approved by:	**SLT**	**4.12.18**
Last Reviewed on:	**27.11.18**	
Next Annual Review due by:	**27.11.19**	

Appendix 1

Social Media Policy

Introduction to Downside School's Social Media Policy for Staff

Downside School is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The most commonly used social networking sites are Facebook, Instagram, snapchat, WhatsApp and Twitter. Communicating content is also increasingly popular using You Tube, Vimeo and Soundcloud.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and with a degree of flexibility, within the spirit of education rather than regulation. Downside now has official pages on all these websites to harness the power to share and endorse content. However, it is also important to ensure that we balance such flexibility with our reputation. In addition, recent changes to KCSIE (Keeping Children Safe in Education) have placed an obligation on schools to ensure that the Staff Code of Conduct must cover staff/pupil relationships and communications including the use of social media.

Our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide a balance to support innovation whilst providing a framework of good practice which is echoed in our Code of Conduct. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of Governing Bodies and the relevant legislation.

Objectives

This policy sets out Downside School's policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for school staff in many ways. This document aims to:

- Assist Downside School staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use.
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Support safer working practice.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Reduce the incidence of positions of trust being abused or misused.
- Ensure that Downside School is not exposed to legal risks.
- Ensure that the reputation of Downside School is not adversely affected.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Head Master or Deputy Head Master of the justification for any such action already taken or proposed.

Scope

This document applies to all who work at Downside School. This includes Monks, Teachers, Support Staff, Supply Staff, Administration Staff, Maintenance Staff, Governors, Volunteers and Contractors. It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in Schools. Reference to pupils means all pupils at Downside School including those over the age of 18.

This policy should not be used to address issues where other policies and procedures exist to deal with them. All Downside School representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Overview and Expectations
All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications. Staff must never post inappropriate, derogatory or abusive remarks or offensive comments which may bring Downside School – or any of its stakeholders - into disrepute.

Social media must not be used by staff to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring Downside School into disrepute.

Social media must not be used to discuss or advise any matters relating to School matters, staff, pupils or parents.

Any member of staff wishing to set up a social media presence in order to:
1. Aid School work or communication in an official manner
2. Promote themselves professionally where the School's name is required

Must inform the Director of External Communications prior to the creation of such an account to ensure continuity and to avoid duplication or any conflict of interest.

Safer Online Behaviour

Managing personal information effectively makes it far less likely that information will be misused.

1. Staff should never publish personal information on social networking sites, such as addresses, home and mobile phone numbers. In addition, a Downside email address should <u>never</u> be associated with a personal social media account.
2. Staff personal profile settings should be set to maximise their privacy, to protect their professional reputation working in a School environment.
3. Twitter users should ensure that their personal profile includes the line: *"This is my personal account (and does not represent the views of Downside School)".* Staff should not follow pupils on Twitter
4. Staff must take all reasonable steps to ensure that their personal information is secure; this means that no pupil should be able to freely search for or access their details. Staff should ensure that any

inappropriate photographs are deleted from any profile.

5. Staff should not be 'Friends' with, 'Followers' of, or connect with pupils on any social media network. It would be considered inappropriate to connect with pupils on a personal account. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers.
6. Staff using Twitter in their official capacity can be followed by pupils but must ensure that content complies with the Staff Code of Conduct at all times and the School Policy on the use of images.
7. Staff should never post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

Digital/mobile communication between Pupils / Downside Staff

Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

All communications between staff and pupils via social media will be performed using an account which is not the member of staff's personal account. If a member of staff is unsure how to set up a business/professional account they should first gain permission from the Deputy Head Master and then seek guidance from the External Communications department.