

E- SAFETY AND CYBERBULLYING POLICY

Introduction

The school recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

Aims

The aims of this policy are to ensure that:

1. Pupils, staff and parents are educated to understand what Cyber bullying is and what its consequences can be
2. knowledge, policies and procedures are in place to prevent incidents of Cyber bullying in school or within the school community
3. we have effective measures to deal effectively with cases of Cyber bullying
4. we monitor the effectiveness of prevention measures

What is E-Safety?

- Effective E-safety requires the knowledge to guard against
 - Identity Theft online
 - Virus and spyware
 - Online 'stranger danger'

Delivery of this requires the education of all the pupils and staff, as well as the establishment of safety innovations such as web filtering, and anti-virus software

What is Cyber bullying?

- Cyber bullying is the use of ICT, commonly a mobile 'phone or the internet, deliberately to upset someone else.
- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying
- It can also go further in that it can invade home/personal space and can involve a greater number of people
- It can take place across age groups and school staff and other adults can be targeted
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'Cyber stalking'; vilification/defamation; exclusion or peer rejection;
- impersonation; unauthorised publication of private information or images ('happy-slapping'); and manipulation

PREVENTING CYBER BULLYING AND PROMOTING E-SAFETY

Understanding and discussion

- The Deputy Head Pastoral is responsible for overseeing the practices and procedures outlined in this policy and for monitoring its effectiveness.
- Staff will receive training in identifying Cyber bullying and understanding their responsibilities in developing e-safety. The Deputy Head Pastoral may delegate this training to the head of PSHE or the LTC IT department as appropriate. In this

LVS ASCOT

training all staff will be helped to keep up to date with the technologies that children are using. (CEOP training delivered 2009, and Deputy Head Pastoral delivered INSET Summer 2010)

- It is made clear in staff meetings that staff should not have contact with current pupils on social networking sites (specifically should not be-friend pupils on Facebook). In addition it is advisable not to have past pupils as friends.
- The delivery of PSHE is important and will discuss keeping personal information safe and appropriate use of the internet.
- It is desirable that the pupils will be involved in developing e-safety and a response to Cyber bullying. They will have a voice through the School Council
- Pupils will be educated about e-safety and Cyber bullying through a variety of means: assemblies, conferences, Anti-bullying Week, projects (ICT, PSHE, Drama, English), etc.
- Pupils (from Y7) and pupils& parents (from Y1) will sign an Acceptable Use Policy before they are allowed to use school computer equipment and the internet in school and parents will be asked to confirm that they have discussed its contents with their children
- Parents will be provided with information and advice on e-safety and Cyber bullying via literature, talks, etc.
- Parents will be provided with information and advice on the legalities of contractual agreements with web companies and organisations (for example Gencon communications with regards permissions with online pics for the web)
- Pupils and staff will be involved in evaluating and improving policies and procedures

Policies and practices

- Ensure regular review and update of existing policies to include Cyber bullying where appropriate
- Provide opportunities for policies to be addressed and for children to be involved in the process of updating and improving them
- Keep good records of all Cyber bullying incidents
- Keep AUPs under review as technologies develop
- Publicise rules and sanctions effectively
- The LTC IT department will use filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the pupils.

Promoting the positive use of technology

- Make positive use of technology across the curriculum
- Use training opportunities to help staff develop their practice creatively and support pupils in safe and responsible use
- Explore ways of using technology to support assertiveness, self-esteem and to develop friendships
- Ensure all staff and children understand the importance of password security and the need to log out of accounts

Making reporting easier

- Ensure staff can recognise non-verbal signs and indications of Cyber bullying with regular CP update training.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement

LVS ASCOT

- Publicise to all members of the school community the ways in which Cyber bullying can be reported
- Provide information for all students including reassurances about 'whistleblowing' and the appropriate way of informing appropriate staff or parents about incidents they have witnessed
- Provide information on external reporting routes e.g. mobile phone company, internet service provider, ChildLine, CEOP or the NSA

RESPONDING TO CYBER BULLYING

Most cases of Cyber bullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within incidents of bullying are investigated. However, some features of Cyber bullying differ from other forms of bullying and may prompt a particular response. The key differences are:

- impact: the scale and scope of Cyber bullying can be greater than other forms of bullying
- targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets
- location: the 24/7 and anywhere nature of Cyber bullying
- anonymity: the person being bullied will not always know who is bullying them
- motivation: some pupils may not be aware that what they are doing is bullying
- evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence
- it is possible that a member of staff may be a victim and these responses apply to them too

Support for the person being bullied

- Offer emotional support; reassure them that they have done the right thing in telling
- Advise the person not to retaliate or reply. Instead, keep the evidence and take it to their parent or a member of staff
- Advise the person to consider what information they have in the public domain
- Unless the victim sees it as a punishment, they may be advised to change e.g. mobile phone number
- If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and make a report to get the content taken down.
- In some cases, the person being bullied may be able to block the person bullying from their sites and services. Appendix 1 contains information on what service providers can do and how to contact them

Investigation

- Members of staff should contact the Deputy Head Pastoral in all cases
- Staff and pupils should be advised to preserve evidence and a record of abuse; save phone messages, record or save-and-print instant messenger conversations, print or produce a screenshot of social network pages, print, save and forward to staff whole email messages
- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact: the local police or CEOP (<http://www.ceop.gov.uk/>)

LVS ASCOT

- Identify the bully. See Appendix 2 for guidance
- Any allegations against staff should be handled as other allegations following guidance in Safeguarding Children and Safer Recruitment in Education.
- Confiscate mobile phone if appropriate
- Contact the police in cases of actual/suspected illegal content

Working with the bully and applying sanctions

The aim of the sanctions will be:

- to help the person harmed to feel safe again and be assured that the bullying will stop
- to hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour
- to demonstrate to the school community that Cyber bullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly
- Sanctions for any breaches of AUPs or internet/mobile phone agreements will be applied
- In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation
- The outcome must include helping the bully to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the bully to change
- Each of the LVS schools will follow its own disciplinary procedures and its own Anti-Bullying Policy

A key part of the sanction may well involve ensuring that the pupil deletes files.

Evaluating the effectiveness of prevention measures

- Identify areas for improvement and incorporate children's ideas
- It is desirable to conduct an annual evaluation including a review of recorded Cyber bullying incidents, a survey of pupil and staff experiences and a parent satisfaction survey
- It is also desirable to publicise evaluation findings; celebrate what works and what improvements are planned

Legal duties and powers

- The school has a duty to protect all its members and provide a safe, healthy environment
- School staff may request a pupil to reveal a message or other phone content and may confiscate a phone;
- If they consider that a mobile phone may contain evidence of bullying or a crime or the potential of a crime they may investigate the specific contents relating to that act.
- Some Cyber bullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997.

For further references please refer to the LVS Anti-Bullying Policy

Reviewed November 2011

Reviewer C Cunningham-Watson, H Donnelly

LVS ASCOT

This policy must be reviewed no later than: December 2012

APPENDIX 1

When and how to contact the service provider:

Mobile Phones

All UK mobile operators have nuisance call centres set up and/or procedures in place to deal with such instances. The responses may vary, but possibilities for the operator include changing the mobile number of the person being bullied so that the bully will not be able to continue to contact them without finding out their new number. It is not always possible for operators to bar particular numbers from contacting the phone of the person being bullied, although some phone handsets themselves do have this capability. Action can be taken against the bully's phone account (e.g. blocking their account), only with police involvement.

Details of how to contact the phone operators:

O2: 08705214000 or ncb@O2.com

Vodafone: call customer services on 191 from a Vodafone phone or on any other phone call 08700700191 for Pay Monthly customers or on 08700776655 for Pay As You Go customers.

T-Mobile: call customer services on 150 from your T-Mobile phone or on 0845 412 5000 from a landline, or email using the 'how to contact us' section of the T-Mobile website at www.tmobile.co.uk

Social networking sites (e.g. Facebook, Bebo, MySpace, Piczo)

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to for all to see. The user can also set their profile to "Private", so that only those authorised by the user are able to access and see their profile.

It is good practice for social network providers to make reporting incidents of Cyber bullying easy, and thus have clear, accessible and prominent reporting features. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social networking sites do receive reports about Cyber bullying, they will investigate and can remove content that is illegal or breaks their terms and conditions in other ways. They may issue conduct warnings and they can delete the accounts of those that have broken these rules. It is also good practice for social network providers to make clear to the users what the terms and conditions are for using the service, outlining what is inappropriate and unacceptable behaviour, as well as providing prominent safety information so that users know how to use the service safely and responsibly.

Contacts for some social network providers:

- facebook and Bebo: reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left hand corner of screen) on every Bebo profile. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a 'Report

LVS ASCOT

Abuse' link located below the content they wish to report. Users have the option to report suspicious online activity directly to the police by clicking the 'Report Abuse' link and then clicking the 'File Police Report' button.

- MySpace: reports can be made via the 'Contact MySpace' link, which is accessible at the bottom of the MySpace homepage (<http://us.myspace.com>), and at the bottom of every page with the MySpace site.
- Piczo: reports can be made within the service (there is a 'Report Bad Content' button at the top of every member page). At the bottom of the home page and on the 'Contact Us' page there is a link to a 'Report Abuse' page. The 'Report Abuse' page can be found at <http://pic3.piczo.com/public/piczo2/piczoAbuse.jsp>.

Instant Messenger (IM)

It is possible to block users, or change Instant Messenger IDs so the bully is not able to contact their target any more. Most providers will have information on their website about how to do this. In addition, the Instant Messenger provider can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations and most IM providers allow the user to record all messages.

It is also good practice for Instant Messenger providers to have visible and easy-to-access reporting features on their service.

Contacts of some IM providers

- MSN: when in Windows Live Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse' and there is also an online feedback form at <http://support.msn.com/default.aspx?mkt=en-gb> to report on a
- Range of products including MSN Messenger.
- Yahoo!: when in Yahoo! Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse.'

Email providers (e.g. hotmail and Gmail)

It is possible to block particular senders and if the bullying persists and alternative is for the person being bullied to change their email addresses. The email provider will have information on their website and how to create a new account.

Contacts of some email providers

- Hotmail: there is an online contact form at <http://support.msn.com/default.aspx?mkt=en-gb>.
- Gmail: there is an online contact form at https://services.google.com/inquiry/gmail_security4.
- Yahoo! Mail: there is a 'Help' link available to users when logged in, which contains a reporting form.

Video-hosting sites

It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps the most well known of such sites, it is possible to report content to the site provider as inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself.

LVS ASCOT

YouTube provides information on what is considered inappropriate in its terms of service see www.youtube.com/t/termssection5c.

Chat rooms, individual website owners/forums, message board hosts

Most chatrooms should offer the user the option of blocking or ignoring particular users. Some services may be moderated, and then moderators will warn users posting abusive comments or take down content that breaks their terms of use.

APPENDIX 2

Identifying the Bully

Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individuals' phone or hacking into their IM or school email account to send nasty messages.

In cases where you do not know the identity of the bully, some key questions to look at:

- Was the bullying carried out on the school system? If yes, are there logs in school to see who it was? Contact the school IT helpdesk to see if this is possible.
- Are there identifiable witnesses that can be interviewed? There may be children who have visited the offending site and left comments, for example.
- If the bullying was not carried out on the school system, was it carried out on a mobile or a particular internet service (e.g. IM or social networking site)? As discussed, the service provider, when contacted, may be able to take some steps to stop the abuse by blocking the aggressor or removing content it considers defamatory or breaks their terms of service. However, the police will need to be involved to enable them to look into the data of another user.
- If the bullying was via mobile phone, has the bully withheld their number? If so, it is important to record the date and time of the message and contact the mobile operator. Steps can be taken to trace the call, but the mobile operator can only disclose this information to the police, so police would need to be involved. If the number is not withheld, it may be possible for the school to identify the caller. For example, another student may be able to identify the number or the school may already keep records of the mobile phone numbers of their pupils. Content shared through a local wireless connection on mobile phones does not pass through the service providers' network and is much harder to trace. Similarly text messages sent from a website to a phone also provide difficulties for tracing for the internet service or mobile operator.
- Has a potential criminal offence been committed? If so, the police may have a duty to investigate. Police can issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message. This may help identify the bully. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact of behaviour). A new national agency called the Child Exploitation and Online Protection Centre (CEOP) was set up in 2006 to deal with child sexual exploitation, and it is possible to report directly to them online at www.ceop.gov.uk However, it is important to note that it is the

LVS ASCOT

sexual exploitation of children and young people, not Cyber bullying, which forms the remit of CEOP.

Information about Cyber bullying and civil and criminal laws

It is very important for schools to take Cyber bullying seriously. It can be a very serious matter and can constitute a criminal offence. Although bullying or Cyber bullying is not a specific offence in UK law, there are criminal laws that can apply in terms of harassment, for example, or threatening behaviour, or indeed – particularly for Cyber bullying – threatening and menacing communications.

APPENDIX 3

Some Useful Agencies/Resources

Websites and resources that offer support guidance and strategies for children, young people, schools and parents/carers to prevent all forms of bullying:

Anti-Bullying Alliance

This site offers information advice and resources on anti-bullying. It is intended to be a one stop shop where teachers can download assembly materials, lesson ideas and information including those for Anti-Bullying Week. The site brings information, advice and resources together from more than 65 of its members, which include charities ChildLine, Kidscape, Mencap and the Association of Teachers & Lecturers (ATL). It has a site called Hometown for children and young people about dealing with all forms of bullying <http://www.anti-bullyingalliance.org/>

Anti-Bullying Questionnaire

Anti-Bullying Questionnaire that schools can download and use to find out about the prevalence of bullying. Go to the following web page and click on Questionnaire. <http://www.anti-bullyingalliance.org/abawek2005.htm>

Anti Bullying Network

An excellent Scottish Anti-Bullying site based at the University of Edinburgh dedicated to promoting a positive school ethos. It has advice for pupils, teachers, parents, on all aspects of bullying, including homophobic, racist and cyber and good case examples of schools in the region that have tried out various strategies to reduce bullying, organised under specific headings. Schools may find these useful for ideas and to adapt. <http://www.antibullying.net>

Antibully

Provides advice to parents whose children are subject to bullying, to spot the signs, listen to them carefully and praise their courage in wanting to deal with the situation. <http://www.antibully.org.uk/bgbullied.htm>

AboutKidsHealth

A Canadian resource and website being developed at The Hospital for Sick Children, one of the largest paediatric teaching hospitals in the world. It has excellent resources on a

LVS ASCOT

number of topics related to children and young people's emotional health, well being and safety, including behaviour, bullying and a good section on Cyber bullying. <http://www.aboutkidshealth.ca.ofhc/news/FTR/3879.asp>

Antidote

This is a pioneering organisation that seeks to shape a more emotionally literate society through its work with schools. It offers an online schools survey SEELS to enable schools to assess their emotional environment for learning. It also builds capacity for school to deliver SEAL. <http://www.antidote.org.uk>

BeatBullying

A very successful charity that supports borough-based, youth-lead, anti-bullying campaigns. It works with young people and professionals and organises seminars, training courses and conferences. It has an accessible website for young people and schools. It also provides professionals with comprehensive antibullying toolkits. <http://www.beatbullying.org>

British Youth Council

The BYC brings young people together to agree on issues of common and encourage them to bring about change through taking collective action. <http://www.byc.org.uk>

Bullying Online

This provides some useful information on a number of bullying behaviours and strategies to prevent bullying. It offers advice to parents and children. However there is no contact link or "about us" section so we do not really know who is behind the organisation or what they stand for. <http://www.bullyfreeworld.com>

BBC Bullying

This provides links and resources explaining how to stop bullying. It also signposts examples of successful school anti-bullying projects and ideas. For example, see Eastlea Community College in Newham and what young people did themselves to raise money and awareness for a bullying awareness project. <http://www.bbc.co.uk/schools/bullying>

Chatdanger

This gives advice for young people and parents on using Internet Chatrooms safely. <http://www.chatdanger.com>

Children's Express

Children's Express is a UK-wide news agency producing news, features and comment by young people for everyone. It encourages young people to express their views through story, journalism, photos and images on all issues including bullying that affect them. It also publicises what the Children's Commissioner is doing for children. www.childrens-express.org

CEOP: (Child exploitation online protection)

A newly formed government agency that is dedicated to promoting online safety for children who may be vulnerable to sexual exploitation in chat rooms. It works with a number of charities and police across the UK and has a website for secondary age pupils called 'thinkuknow'. <http://www.ceop.gov.uk/>

LVS ASCOT

ChildLine

This provides a 24 hour helpline for children and young people being bullied in the UK. Children and young people can call 0800 1111 to talk about any problem. It is a major charity that is now housed with NSPCC. It provides training in peer support for pupils and schools and has a range of publications and downloadable resources for children, parents and teachers. <http://www.childline.org.uk>

Childnet International

This is a charity that aims to make the internet a safer place for children and is dedicated to internet safety. It is concerned to prevent abuse on the internet and cyber bullying. It has advice for children and parents and has some useful resources for teachers of ICT at key Stage 3 on internet safety. It is located in South London (Brockley). <http://www.childnet-int.org>

Children's Legal Centre

This has produced a very helpful document called 'Bullying-a Guide to the Law' which can be downloaded. This publication is an essential tool for parents whose children are being bullied and for professionals providing advice in this area. It advises on actions schools are required to take to prevent and deal with bullying effectively, as well as providing practical advice on what parents can do if a school fails to support their child. <http://www.childrenslegalcentre.com>

Commission for Racial Equality

This has examples of anti-harassment policies and links for education establishments to websites that provide relevant information on racist aspects of bullying. <http://www.cre.gov.uk>

Kidscape

Kidscape is committed to keeping children safe from abuse. It is the first charity in the UK established specifically to prevent bullying and child sexual abuse it provides information, good resources and training for children and young people under the age of 16, their parents/carers. It offers a range of courses for professionals. It also provides courses in assertiveness training, ZAP, for children and young people and develops their confidence and skills to resist bullying and forms of abuse. <http://www.kidscape.org.uk>

NSPCC

The NSPCC works tirelessly and promotes public campaigns to stop cruelty to children. There is advice on a number of issues related to bullying, child protection, and abuse. Kids Zone which contains details for their child protection helpline for young people who have problems at home or are being bullied. <http://www.nspcc.org.uk>

Bullying and Disability

Factsheet produced by the Bullying Task Force of the Transition Information Network (TIN), an alliance of organisations and individuals who come together with a common aim: to improve the lives and experiences of disabled young people's transition to adulthood. The factsheets on bullying and disability provides some insight into the different types of bullying and how the law can help stop bullies. Available at: www.bullyingtaskforce.org/doc/infosheet_pt1.doc
http://www.bullyingtaskforce.org/doc/infosheet_pt2.doc

LVS ASCOT

Bullying around Racism, Religion and Culture

This advice for schools is the first in a suite of specialist guidance on countering prejudice-driven bullying in schools. This advice was created with the help of children and young people, Head teachers and staff, community and voluntary sector organisations, professional associations and local authority officers. Available at: <http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/racistbullying>

Books

Most of the websites listed above have books and resources that schools can order to extend their understanding of bullying and how to prevent it.

Journeys

Children and young people talking about bullying. This booklet, the first publication from the Office of the Children's Commissioner for England, tells the real stories of ten children and young people who have experience bullying. It also includes their tips for dealing with bullying and an endnote by Al Aynsley-Green, the Children's Commissioner for England. Available at: <http://www.anti-bullyingalliance.org.uk/pdf/journetsa4.pdf>

Primary

"A Volcano in my Tummy" written by Elaine Whitehouse and Warwick Pudney. The book begins with a little insight into anger itself as well as the "rules" of anger. Anger is okay. It's okay to feel anger, to talk about anger, to express anger in an appropriate way. It's not okay to hurt yourself and other people, animals or things when you are angry. This is an excellent practical resource with imaginative ideas for lessons to help children to manage and deal with the emotion of anger. www.amazon.co.uk

Secondary

Adolescent Volcanoes. Is another marvellous book that has a section for adolescents and one for adults giving useful activities and exercises that can be adapted to help young people to deal with anger, set boundaries and communicate appropriately.

APPENDIX 4

Reports, Training Materials and Strategies to reduce bullying:

Reports by Ofsted and HMI that summarize practice and indicate ways forward:

1. Bullying: Effective action in secondary schools (2003). A report by Ofsted see website – <http://www.ofsted.gov.uk>
2. Recent and very good. 'Tackling Bullying in schools'. A survey of effective practice June (2006). This is a lively and very useful report on strategies schools use to prevent bullying, highlighting good practice case examples from Her Majesty's Inspectors in Education and Training in Wales. It can be downloaded from: http://www.estyn.gov.uk/Publications/Remit_Tackling_Bullying_in_schools_survey_of_effective_practice.pdf
3. Another report from ESTYN on good practice in managing behaviour in schools is also relevant (July 2006) http://www.estyn.gov.uk/Publications/Remit_Tackling_Bullying_in_schools_survey_of_effective_practice.pdf

LVS ASCOT

DCSF Suite of Guidance

Safe to Learn

- Bullying Around Race Religion and Culture
- Cyber bullying
- Homophobic Bullying
- Bullying of Children with Special Needs and Disabilities.

Primary and Secondary National Strategies

Social and Emotional Aspects of Learning (SEAL)

Primary Materials 'Say No to Bullying'

An archive of PDFs providing guidance on the theme 'Say no to bullying', forming part of SEAL Excellence and Enjoyment. Includes guidance on staffroom and family activities, the Foundation Stage and Years 1 to 6

Nationalstrategies.standards.dcsf.gov.uk/node/89185?uc=force_uj

Secondary National Strategy

SEAL: Anti Bullying Resource for Secondary Schools

It includes a theme overview

- A set of structured staff development opportunities.
- Ten example learning opportunities for use with pupils in Years 7.8 and 9 that can be delivered flexibly to promote progression or to develop specific skills according to needs. These flow from a series of stimulus materials. They are divided into three themes: individuals, resilience and bullying; group bullying; prejudice-driven bullying: Nationalstrategies.standards.dcsf.gov.uk/node/66375

Healthy Schools

<http://www.healthyschools.gov.uk>

The accreditation guidance for Healthy schools especially in relation to emotional health and well being (EHWB) and how this impacts on bullying. Anti-Bullying Guidance was published from Healthy Schools in November 08

Inside Justice Week (18-25 November)

Shows people how they can help deliver justice and why it matters. Schools up and down the country have participated in the campaign in previous years, running mock trials, attending events at local courts and police stations, and even welcoming the local police into their classes.

LVS ASCOT

ADDITIONAL APPENDIX – GUIDANCE NOTES FOR COMPUTER ACCEPTABLE USE POLICY

Contents

APPENDIX 1	14
Guidance notes on the use of email, internet and networks	14
1. Use of school email is encouraged	14
2. Email is to be used for school-related and professional purposes only (with specific exceptions listed below)	14
3. Email is not routinely monitored either on a regular or spot check basis. 14	
4. There are some recommended rules for communicating via email, forums or social networking.	15
5. User responsibilities	15
6. General security	17
APPENDIX 2	18
General guidance on Spyware and Viruses.....	18
Spyware Cleaning.....	18
Viruses	18
Update of spyware signature files, virus signature files and engine .	18
APPENDIX 3	19
General advice on protecting yourself online and dealing with Cyber bullying.....	19
To avoid the risk of being exposed to illegal content and protecting yourself online, we recommend the following precautions:	19
General advice on how to deal with Cyber bullying	19

APPENDIX 1

Guidance notes on the use of email, internet and networks

1. Use of school email is encouraged

The school encourages the use of email for work related activities and respects the privacy of users.

2. Email is to be used for school-related and professional purposes only (with specific exceptions listed below)

The School accepts that there may be some exceptions to the above restrictions:-

Urgent or emergency emails. Taking a common sense analogy of phone usage, the urgent or emergency email would include anything that you would normally expect to be allowed to conduct by phone.

Use of school computing resources for personal use is allowed as follows:

During school days but in students own time (non-school time)

Any time during non-school days (except where explicitly detailed by staff)

3. Email is not routinely monitored either on a regular or spot check basis. However, the school reserves the right to monitor email under specific circumstances

The school does not routinely inspect, monitor, or disclose email without the users consent. Nonetheless, subject to the requirements for authorisation (specified below), the school may deny access to its email services and may inspect, monitor, or disclose email where such activities are required to carry out the following:

Preventing or detecting criminal activity

Preventing the unauthorised use of the computer systems - i.e. ensuring students do not breach the schools acceptable use policy

Recording evidence of business transactions

To ensure compliance with regulatory or self-regulatory guidelines

To allow the maintenance or the effective operation of the schools systems (e.g. preventing viruses or spam, or users persistently turning computers off)

In order to conduct any investigations, prior approval is required from any one of the following:-

Headmistress LVS Senior School

Head Teacher LVS Junior School

Head Teacher LVS Hassocks School

LVS ASCOT

4. There are some recommended rules for communicating via email, forums or social networking.

When using any tool for sending messages on or via a computer network, be sure to use formality appropriate for the situation and realise that digital communications, like print, is permanent.

To use digital communication effectively, you should know the basics of netiquette - etiquette on a network.

Take some care with your writing. Although these forms of communicating are informal, do not embarrass yourself by sending messages that you have not proofread. Text-editing functions on these other communication systems are more limited than on Word. Use uppercase and lowercase letters as you do in other forms of correspondence - UPPER CASE LOOKS AS IF YOU ARE SHOUTING.

Skip lines between paragraphs.

Email should have a subject heading which reflects the content of the message.

If you think the importance of a message justifies it, immediately reply briefly to the message to let the sender know you have received it, even if you will send a longer reply later.

Do not send large amounts of unsolicited information to people, like jokes, attached video clips or series of pictures.

Messages and articles should be brief and to the point. Don't wander off-topic, don't ramble and don't send messages solely to point out other people's errors in typing or spelling. When someone makes a mistake - whether it is a spelling error, a stupid question or an unnecessarily long answer - be kind about it. If it is a minor error, you may not need to say anything.

Avoid sending messages or posting articles which are no more than gratuitous replies to replies.

When quoting another person, edit out whatever is not directly applicable to your reply. Don't let your mailing automatically quote the entire body of messages you are replying to when it's not necessary. Take the time to edit any quotations down to the minimum necessary to provide context for your reply. Nobody likes reading a long message in quotes for the third or fourth time, only to be followed by a one line response: "Yeah, me too."

Pay attention. Read all outgoing email carefully, checking for errors in both grammar and spelling. Be professional and careful what you say about others. Email is easily forwarded!

5. User responsibilities

This Policy specifies the actions allowed and prohibited by users of the School's email and internet services.

By using our services you agree to comply with our policies. You are expected to use the services with respect, courtesy, and responsibility, giving due regard to the rights of other service users. We expect you to have a basic knowledge of how the service functions, the types of uses that are generally acceptable and the types of uses that are to be

LVS ASCOT

avoided. Common sense is the best guide as to what is considered acceptable use. The following are unacceptable uses:

Illegality in any form, including but not limited to activities such as unauthorized distribution or copying of copyrighted software (which include freeware, shareware and public domain software) or other copyrighted material, harassment, fraud, trafficking in obscene material, drug dealing, violation of U.K. export restrictions, and other illegal activities.

The provisions of this Policy are intended as guidelines and are not meant to be exhaustive. Generally, conduct that violates law, regulation, or the accepted norms of the Internet community, whether or not expressly mentioned in this Policy, is prohibited.

The user acknowledges that the School is unable to exercise control over the content of the information passing through the School's Network. Therefore, the Charity or Schools are not responsible for the content of any message whether or not the posting was made by a user of the School.

The user may not circumvent user authentication or security of any host, network, or account (including "cracking", "hacking" or "proxy avoidance"), nor interfere with service to any user, host, or network (including "denial of service attacks").

Violations of system or network security are prohibited, and may result in criminal and civil liability. The School will investigate incidents involving such violations and will involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include (without limitation) the following:

Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;

Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network;

Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

Forging or manipulation of data, to any ill means

When the School becomes aware of an alleged violation of this Policy, a thorough investigation will be undertaken. During the investigation the School may restrict users' access in order to prevent further possible unauthorised activity. Depending on the severity of the violation, the School may, at its sole discretion, restrict, suspend, or terminate users account and/or pursue other civil remedies. If such violation is a criminal offence, the School will notify the appropriate law enforcement department of such violation.

It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam mail") of any kind (commercial advertising, political tracts, announcements. etc.).

It is also explicitly prohibited to allow others to send unsolicited bulk mail messages either directly or by relaying through the Users systems. Users may not forward or propagate chain letters nor malicious email.

A user may not solicit mail for any other address other than that of the user, except with full consent of the owner of the referred address.

LVS ASCOT

You shall be held liable for any and all costs incurred by the School as a result of your violation of these terms and conditions.

6. General security

Password security

Password security is advised to be at least 8 characters in length and consist of both alphabetical and numerical characters. Each user will be asked to changed their password after a specific length of time, with the computers giving 14 days notice of their password expiring.

Unattended PCs

Users shall not leave a PC unattended. If a user needs to leave a PC for a short period of time, ensure that you have LOCKED the PC (*Activated by pressing <CTRL-ALT-DELETE> keys together and clicking the “LOCK workstation” button*).

If you must leave the PC unattended for a lengthy period of time please ensure that you save all current documents and close all applications before “**LOGGING-OFF**” the PC.

PLEASE NOTE: Any person utilising a shared computer who leaves it in a LOCKED state for a lengthy period of time, will find that a systems administrator policy will log the machine off, effectively loosing all work open in the current session. (Please have consideration for other users, as well as the security of information).

Breaches of School policies can result in disciplinary action being taken, up to and including dismissal or expulsion.

APPENDIX 2

General guidance on Spyware and Viruses

Spyware Cleaning

SPYWARE is a generic term typically describing software whose purpose is to collect demographic and usage information from your computer, usually for advertising purposes. The term is also used to describe software that 'sneaks' onto the system or performs other activities hidden to the user. Spyware applications are usually bundled as a hidden component in mislabelled "freeware" and shareware applications downloaded from the Internet. A spyware module may be active on your computer at this moment without your knowledge. These modules are almost always installed on the system secretly, suggesting that spyware companies know how users feel about such software and figure that the best and only way to ensure its widespread use is to prevent the end-user from discovering it.

The charity and school's use a combination of software from McAfee, Microsoft, Ironport and other parties to protect our networks.

Viruses

You must prevent intentional intrusions into your computer and network that take the form of viruses. Follow these tips to help prevent virus outbreaks.

You can unwittingly bring viruses into the network by loading a program from a source such as the internet, instant messaging, email attachments or removable storage device (e.g. USB key, firewire hard drive, SD card or optical media).

Learn the common signs of viruses: unusual messages that appear on your screen, decreased system performance, missing data, and inability to access your hard drive. If you notice any of these problems on your computer, run your virus-detection software immediately to minimise the chances of losing data.

Programs on USB keys or other removable media may also contain viruses. Scan all media before copying or opening files from them, or starting your computer from them.

You can run McAfee VirusScan Enterprise (which is installed on your computer) regularly to check your computer for viruses. However! Your laptop is configured to scan your local hard disks every day.

Update of spyware signature files, virus signature files and engine

Your system is set to automatically download the updates from the network. If you have a laptop and have not connected to the network for any period longer than a week, please ensure you contact the IT helpdesk, to obtain a recent update before reconnecting to the network.

Warning: Non-compliance with this procedure, is liable to cause damage to the network and its' users. It is your responsibility to attain standards in compliance with this policy.

APPENDIX 3

General advice on protecting yourself online and dealing with Cyber bullying

To avoid the risk of being exposed to illegal content and protecting yourself online, we recommend the following precautions:

- Do not share your personal information! This includes pictures of you or your family and friends, email addresses, mobile numbers and online IDs.
- Do not arrange to meet strangers! You may have been communicating with people you think you know online, but do you really know who they are?
- Do not open email or links on social networking pages from people you do not know or when you do not recognise the email address
- Similarly, do not open attachments or pictures you receive from unknown people or email addresses
- Ensure you have an effective filter on your PC to stop unwanted content.
- If you are regularly using search engines (such as Google, Bing or Yahoo), you can set each search engine site to a strict level of filtering. This limits what a search will bring up when entering keywords. Check your options with your preferred search engine site. Once you have chosen a search filtering level, check these settings regularly to ensure they have not been amended or switched off.
- Viewing illegal images online can carry a penalty of up to 10 years in prison in the UK.
- Curiosity is normal on the internet, but being exposed to unwanted and potentially illegal images is not acceptable.
- Child Abuse images reflect just that; abuse of children and as such, should always be reported.

Did you know that the age of criminal responsibility starts at age 10 in England and Wales!

General advice on how to deal with Cyber bullying

Due to the anonymous nature of digital communication, anyone with a mobile phone or internet connection can be the target of Cyber bullying. Our schools have clear policies on dealing with bullying and Cyber bullying, please contact the schools or view our websites for a copy of these policies.

Here are some general points to help deal with Cyber bullying:

- If you feel you are being bullied by email, text or online, do talk to someone you trust.
- Never send any bullying or threatening messages.
- Keep and save any bullying email, text or images.
- If you can make a note of the time and date bullying messages or images were sent and note any details about the sender.
- Use blocking software; you can block instant messages from certain people, “unfriend” people on social networking sites or use mail filters to block email.

LVS ASCOT

- **Do not** reply to bullying or threatening messages or emails; this could make matters worse. It also lets the bullying people know that they have found a “live” number, email address or “active” social networking contact.
- **Do not** give out your personal details online; if you are in a chatroom, online game or IM session watch what you say about where you live, the school you go to, your email address, your friends and family. All these things can help someone build up a picture about you.
- **Do not** forward abusive texts, email or images to anyone. You could be breaking the law just by forwarding them. If they are about you, keep them as evidence.
- **Do not ever** give out passwords!
- **Remember** that sending abusive or threatening messages is against the law.
- **Do** report instances of Cyber bullying you have seen or heard about, even if not directed at you. There is no such thing as an innocent bystander, if you have seen the posts, messages or images then you could be considered as part of it if you do not report it!

Have you seen this symbol on the sites you use?



It is your door to one stop internet safety advice and help. If you use social networking areas or other sites offering chat or contact with online buddies then look for it. It is there for you!

Reviewed **January 2012**

Reviewed by **C Cunniffe/C Cunningham-Watson**

Next review **January 2013**