LIMPSFIELD GRANGE SCHOOL

*'together we make a difference'*

# Online Safety Policy

# (Formerly E-Safety)

***This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment***

| | |
|---|---|
| **Governor's Committee Responsibility:** | **Curriculum and Student Welfare** |
| **Date Approved:** | **Autumn Term 2018** |
| **Review Period:** | **Annually** |
| **Next Review Date:** | **Autumn Term 2019** |

## The Limpsfield Grange Values:

At Limpsfield Grange we believe in working together to make a difference.

We are a tolerant community; we accept, value and understand others.

We care for all members of our community without judgement.

We are responsible for our own learning, behaviour and actions.

We accept that sometimes things go wrong. We work together to take responsibility for our mistakes and for putting things right.

We are a respectful community and we treat others as we would like to be treated, even if they have different views and opinions to our own.

We understand that good behaviour helps us to prepare for life beyond Limpsfield Grange.

We are positive and resilient. We celebrate difference in everything that we do.

We are all proud to be part of the Limpsfield Grange community.

*July 2017*

# Limpsfield Grange School Online Safety Policy

**Background and rationale**

Limpsfield Grange's Online Safety policy aims to create an environment where students, staff, parents, Governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Internet technology helps young people learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety policy encourages appropriate and safe conduct and behaviour when achieving this.

Students, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.

These agreements and their implementation will promote positive behaviour which can transfer directly into each young person's adult life and prepare them for experiences and expectations in the workplace.

**Ofsted have identified three areas of online safety in relation to students**

- Being exposed to illegal, inappropriate or harmful material
- Being subjected to harmful online interaction with other users
- Personal online behaviour that increases the likelihood of, or causes, harm

**Aims of this policy**

- For all groups of students to feel safe at school, that they understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe.
- To promote a real world, responsible and positive outlook towards Digital Literacy and online safety aimed at preparing students for expected standards of behaviour in adult life and the workplace.
- To ensure that this policy is closely integrated with other relevant policies and procedures including Safeguarding, Staff Behaviour policy, Procedures for accessing school email on handheld devices, Online Safety Rules (students) and Guidance for the promotion of respect, tolerance, socially acceptable behaviour and developing responsible citizens (formerly the Anti Bullying Policy.)

**Scope**

This policy applies to all users of ICT on the school site including students, staff, parents, Governors, visitors and contractors.

It also covers the following:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including social media and the school website.
- School ICT equipment off-site, for example staff laptops and digital cameras.
- Students and staff personal ICT equipment (when used in school) that makes use of school networking, file-serving or Internet facilities.
- Mobile phones, devices and laptops when used on the school site.

.

**Procedures**

Limpsfield Grange will:

- Ensure all students and staff understand online safety issues and make online safety a school priority.
- Provide education and training to promote knowledge and safe use of the Internet and social media.
- Work with families to help them ensure that young people use the Internet, social media and new technologies safely and responsibly both at home and at school.
- Teach students to be critically aware of the materials they read and show them how to validate information before accepting its accuracy.
- Use students' views to develop online safety strategies.
- Help students to understand how to manage risk and bridge the gap between systems at school and the more open systems outside school.
- As part of the remit of the Online Safety Committee systematically review and develop online safety procedures, including training, to ensure that they have a positive impact on students' knowledge and understanding.
- Ensure students are aware of online safety reporting procedures in school and how to use the CEOP Report Abuse icon.
- Ensure that clear and transparent procedures exist for monitoring, logging and reporting incidents.

Monitoring the online safety policy:

The online safety policy will be actively monitored and evaluated by the following people:

- Online Safety Co-ordinator (Student Support Lead)
- Designated Safeguarding Lead (Head of Residential Provision)
- Senior Leadership Team
- Online Safety Committee members

The online safety policy will be monitored through

- Termly meetings of the Online Safety Committee
- Lesson drop ins and observations
- Weekly monitoring of suspicious Internet searches
- Regular and ongoing monitoring of Internet use through Lightspeed reporting
- Weekly Senior Leadership Team meetings
- Regular monitoring by the Online Safety Co-ordinator
- Headteacher reports to Governors
- Governor visits
- Standard 20 visits and reports in the Residential Provision
- Ofsted inspections (Education and Residential)

Online Safety Policy review and evaluation schedule:

The Online Safety Policy is reviewed annually, and additionally in the case of the following:

- Serious and/or frequent breaches of the Online Safety Rules, Staff Behaviour policy or other in the light of online safety incidents.
- New guidance by Government/ LA /Surrey Safeguarding Board / Ofsted
- Significant changes in technology used by the school or students in the wider community

- Online safety incidents in the community or local schools which might impact on the school community
- Advice from the Police

The Online Safety Co-ordinator:

The school has a designated Online Safety Co-ordinator (Sam Janaway -Student Support Lead) who reports to the Headteacher and coordinates online safety provision across the school and wider school community.

The role of the Online Safety Co-ordinator includes:

- Ensuring all staff are aware of their responsibilities and the school's online safety procedures
- Promoting best practice in online safety within the wider school community, including providing information for parents.
- Participating in the online safety committee meetings
- The Online Safety Co-ordinator is trained in specific online safety issues (CEOP accredited course).

The Designated Safeguarding Lead:

- The Designated Safeguarding Lead will consult with the Senior Leadership Team and Online Safety Co-ordinator to decide which incidents are reported to CEOP, Local Police, LADO, Social Services and parents/carers; and also determine whether the information from such an incident should be restricted to nominated members of the Senior Leadership Team.
- Maintaining a log of submitted online safety reports and incidents

Possible scenarios might include:

- Allegations against members of staff
- Computer crime – for example hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of online bullying in the form of threats of violence, harassment or a malicious communication
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying

The School Business Manager:

- Ensuring staff has signed the Staff Behaviour Policy and all students have signed the Online Safety Rules
- Alerting the Leadership Team of day to day online safety issues
- Liaising with LA contacts and SoftEgg ICT support

Staff:

- Online safety training is included in the induction programme for all new staff
- All staff are expected to sign the Staff Behaviour Policy
- All staff need to ensure that they are aware of the current school Online Safety policy, practices and associated procedures for reporting online safety incidents
- Staff need to ensure that they understand the policies relevant to the Internet, social media and computer use in school
- Staff need to follow the school procedures, as set out in the staff handbook in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual

obligations, and conduct on Internet school messaging or communication platforms, for example email and the school website
- Staff are expected to rigorously monitor students' Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site
- Staff should promote best practice regarding avoiding copyright infringement and plagiarism
- Internet usage and suggested websites should be pre-vetted and documented in curriculum planning

Students:

- Are required to use school Internet and computer systems in agreement with the Online Safety Rules. Students are expected to sign these rules to acknowledge their compliance
- Students need to be aware of how to report online safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button
- Students are made aware that the Online Safety rules cover all computer, Internet and gadget usage in school.
- Students are made aware that their Internet use out of school on social networking sites such as Facebook is covered under the Online Safety Rules if it impacts on the school and/or its staff and students in terms of online bullying, reputation or illegal activities

Families and carers:

- The school expects families and carers to support this online safety policy on promoting safe, responsible and appropriate Internet behaviour and use of ICT equipment both at school and at home
- The school makes families and carers aware of the Online Safety Rules and expects these to be upheld regarding their own use of school systems such as websites and social media
- The school provides training for families and carers on online safety

Governors' responsibility for online safety:

- Termly online safety updates are included as part of the Headteacher's report to governors
- The Governor with responsibility for CPD will be responsible for recommending appropriate Governor online safety training

**How will the school provide online safety education?**

- Online safety is taught through our Computing curriculum, how to judge the validity of website information, how to remove online bullying, computer usage and the law, how to spot and remove viruses, why copyright is important
- Online safety as a part of Live Life Well e.g. how to deal with online bullying, how to report online bullying, the social effects of spending too much time online
- Online safety as part of the school's WACI curriculum

Particular behaviour which will be highlighted might include:

- Explaining why harmful or abusive images on the Internet might be inappropriate or illegal
- Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe
- Explaining how accessing and/or sharing other people's personal information or photographs might be inappropriate or illegal

- Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates and how grooming can develop
- Exploring in depth how online bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it
- Teaching students to assess the quality of information retrieved from the Internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines
- Informing students and staff of copyright and plagiarism infringement laws and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally
- Encouraging responsible and effective digital literacy skills which extend beyond school and into the workplace
- The medical and social effects of spending too much time on the internet, games consoles and computers

**Parents – information, presentation, collaborative meetings and events**

- Online safety information directly delivered to parents via letters, newsletter, website, emails, Parentmail

**Staff training**

- Online safety information delivered to staff via posters, newsletters, flyers, emails, website, handover and staff meetings.
- A planned calendar programme on online safety training opportunities to be made available for staff, including onsite INSET, whole staff training and online training opportunities
- The Online Safety Co-ordinator should be the first port of call for staff requiring online safety advice

**Governors – training**

- Online safety information delivered directly to governors via emails, newsletters, school website
- Babcock 4S e-safety training sessions for Governors
- Governors are invited to our annual whole school safeguarding training which include online safety

**Information system security**

**Filtering**

- SoftEgg will be the first port of call for advice regarding filtering, our filtering provider is Lightspeed which is part of the Schools Broadband service.
- Filtering and monitoring needs to reflect real life rather than being a 'locked down' system.
- Students need to be taught positive responsible behaviour to carry forward into the workplace.
- If staff become aware of unsuitable online materials, the site must be reported to the School Business Manager who will share this information with the Designated Safeguarding Lead. If students become aware of unsuitable online materials, the site must be reported to the supervising member of staff.
- Regular checks are in place to test staff and student filtering systems. These checks are carried out by the Designated Safeguarding Lead.
- Games machines that have Internet access may not include filtering. Close supervision will be given to ensure appropriate use of both machine and software within the school.

**Security**

Passwords:

- The school network profiles require users to input a username and password, this enables activity to be monitored in order to fulfil online safety requirements. The Online Safety Co-ordinator keeps a record of student passwords
- The school will use 'strong' passwords

Disposal

All school computer equipment is disposed of using a reputable company that wipes the data and provides the appropriate documentation to prove this has taken place.

Use of IT facilities for curriculum

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites should be suggested and provided by bookmarks.

**Use of images and videos**

In terms of online safety, the school will ensure images and videos of students, staff, student's work and any other personally identifying material must be used, stored, archived and published in line with GDPR, the Data Protection Act, ICO guidance for schools, DFE guidance for schools and the schools Online Safety Rules and Staff Behaviour Policy.

The ICO publishes comprehensive advice for schools, parents and students with regards to GDPR and the Data Protection Act. This advice helps dispel many of the urban myths.

Guide for schools: www.ico.org.uk/for-organisations/education

Advice on taking photographs in schools:

www.ico.org.uk/media/for-organisations/documents/1136/taking_photos.pdf

**Photographs**

- There are no laws preventing the taking of photographs in public spaces, and no permission is required to take photographs in public places. However, on private property such as Limpsfield Grange School, the permission of the Headteacher is required.
- The school will seek to prevent the 'publication' of photographs (or videos) taken on the school site (for example on the Internet), and limit the use of photographs, for example, to home photo albums and there is provision in law to achieve this: http://www.legislation.gov.uk/ukpga/1988/48/section/85 . It needs to be made clear that the school allows the photography of school events providing the parent "agrees to use the image only for private and domestic purposes".
- The school will take "all reasonable steps to prevent identifying information being included with photographs taken on the school site," (the school doesn't reasonably have the means to control any publication off the school site by other schools, event organisers, the press or members of the public).
- Parental permissions collected from all parents/carers at the beginning of the academic year or on admission will include a section on photographs and the Internet. This information will be collated and relevant staff will be given a list for their records. Parents have the right to remove their consent at any time.

- Photographs that include students will be carefully selected and will not enable individual students to be clearly identified.
- Staff must only use school equipment e.g. cameras, video cameras, memory sticks, laptops, memory cards or other storage devices for photographing of students and activities. Any such images should be uploaded and remain on the school premises.
- Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on the appropriateness in terms of content and behaviour; will wear identification at all times and will not have unsupervised access to the students.

**Email**

- **Students and staff may only use approved email accounts on the school system.**
- Students must immediately tell a supervising adult if they receive an offensive email.
- Students must not reveal personal details or the personal details of others in email communications, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via the school email address.
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how emails from students to external bodies are presented and controlled.
- The forwarding of chain letters is not permitted.

**Social networking**

Personal networking tools include blogs, wikis, Twitter, social networking sites, chat rooms and instant messaging programmes.

- The school will control access to social networking sites, and consider how to educate students in their safe use e.g. use of safe passwords and privacy settings
- Newsgroups will be blocked unless a specific use is approved
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harming or defamatory
- Students and parents will be advised that the use of social network spaces outside school brings a range of dangers to all students
- Students will be advised to use nicknames and avatars when using social networking sites

**Video-conferencing and the use of Skype**

- Students should ask permission from the supervising adult before making or answering a video conference or Skype call
- Video-conferencing and Skype will be appropriately supervised according to the students' age

**Mobile phones**

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity, as a tool to help manage anxiety or to assist with life skills using specific apps (e.g. alarm). The sending of abusive or inappropriate text messages is forbidden. Staff are expected to lead by example. Personal mobile phones should be switched off or on 'silent' during

lessons. Staff phones must be kept in bags or in drawers during lessons or times when they are supervising students. Staff are not permitted to use or check their phones during lessons or times when they are supervising students.

- Staff will use a school phone where contact with students and parents is required. If using a personal mobile phone or home telephone we would advise that, wherever possible, staff withhold their number. If circumstances arise that staff need to use their own phones and they cannot withhold their number, a member of the Senior Leadership Team must be informed.

**Data Protection and online safety**

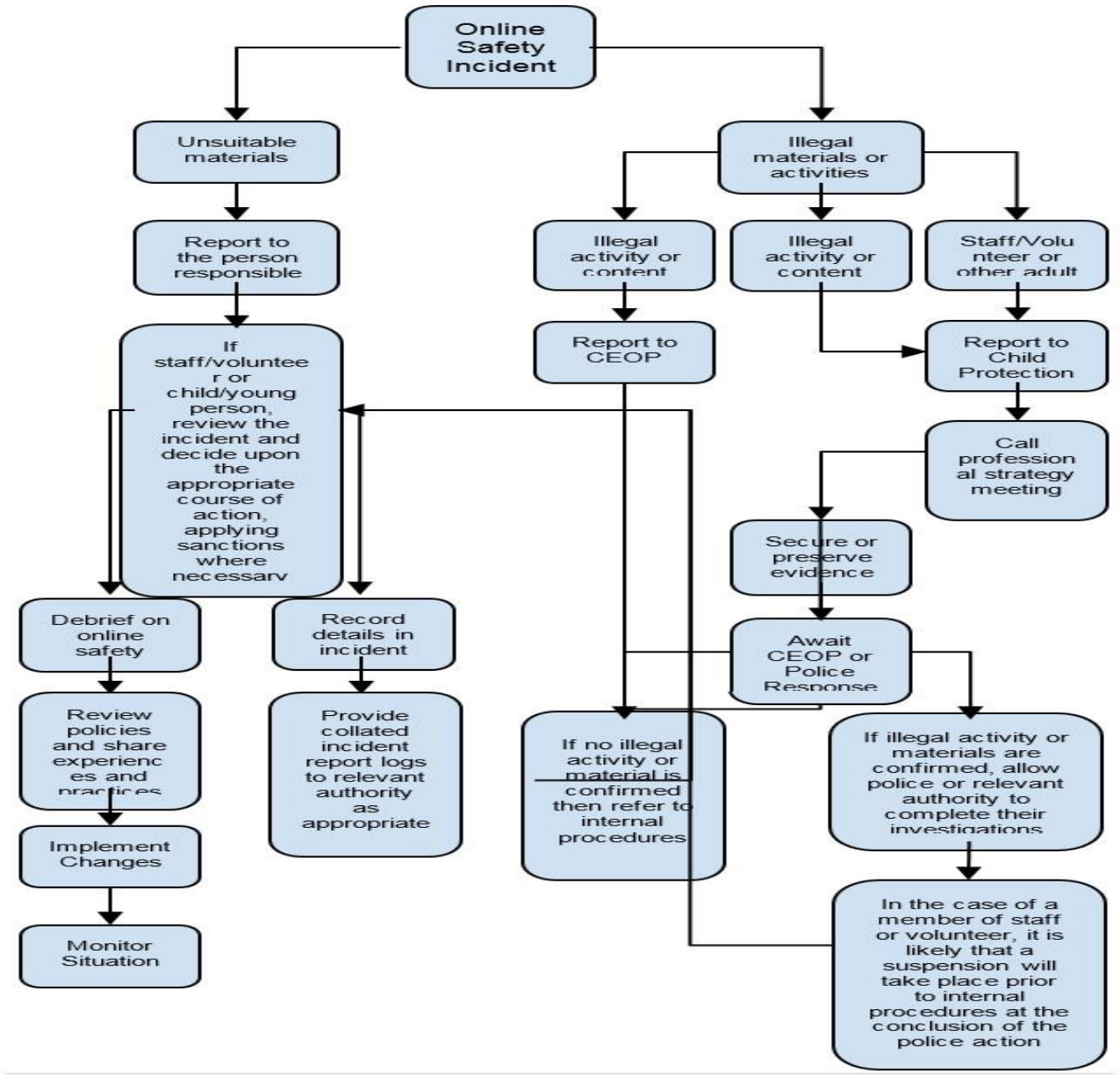
- The General Data Protection Regulations (GDPR) are relevant to online safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
- Staff or students personal information will not be published on the school website.
- Staff will ensure that care is taken to ensure the safety and security of personal data regarding all of the school population
- Personal data will only be stored on secure devices – computers, servers, file-servers, cloud space, or devices which require a user name and password to access the information.
- Secure accounts will be logged off after use to prevent unauthorised access.
- Screen lock to be used (Ctrl/Alt/Delete) when members of staff are away from their desk.
- Any memory stick or pen drive can be converted for encrypted use with free software – http://www.esecurityplanet.com/views/article.php/3880616/How-to-Encrypt-a-USB-Flash-Drive.htm
- However, by far the most effective way to safeguard personal data when off the school site is not to transfer personal information outside school systems if possible
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Online Safety Co-ordinator or a member of the Senior Leadership Team before use in school is granted.

**How to deal with online safety incidents – action to take**

Lightspeed suspicious search reports, which include both student and staff activity, will be printed on a weekly basis and discussed at Senior Leadership Team meetings; appropriate action will be taken as necessary by the Designated Safeguarding Lead and/or other members of the Senior Leadership Team.

Illegal incidents:

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the Police.




Other incidents:

It is hoped that all members of the school community will be responsible users of the digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by students and if necessary can be taken off site by the Police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to a form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by the Local Authority
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **isolate the computer in question as best you can. Any change to its state may hinder a later Police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

**Online safety and the Law:**

Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
General Data Protection Regulations 2018
Freedom of Information Act 2000
Communications Act 2003, sections 1-2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003

The Education and Inspections Act 2006 (Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site. Also, staff can confiscate mobile phones if they cause disturbance and breach the School's Behaviour Policy.

**Copyright Infringement and DMCA:**

If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto sites such as Facebook and Twitter.

**Duty of care and 'in loco parentis':**

Schools have a 'duty of care' to students and as such act 'in loco parentis.' Under the Children Act 1989 this enables schools to remove personal information, online bullying and comments relating to school students as if they were the student's parent. Facebook in particular has provision for using 'in loco parentis' when reporting online bullying.

**Policy review:**

- This policy was approved by the Governing Body of Limpsfield Grange School and is published for viewing by parents and the wider school community on the school website (www.limpsfieldgrange.co.uk)
- The Online Safety policy will be reviewed and evaluated promptly in the light of serious online safety incidents and/or important changes to legislation/Government guidance related to online safety.
- The Online Safety policy will be monitored through termly Online Safety Committee meetings, and through termly updated to the Curriculum Community and Student Welfare Committee
- The Governing Body will receive a report on the progress, evaluation, impact and effectiveness of the Online Safety Policy termly in the Headteacher's Report to Governors. This report will include a synopsis of any online safety incidents and how they have been resolved, listing counter measures implemented.

**Related policies and documents**

- Behaviour Policy
- Child Protection and Safeguarding Policy
- Complaints Policy & Procedures
- Guidance for the promotion of respect, tolerance, socially acceptable behaviour and developing responsible citizens (formerly the Anti Bullying Policy)
- Online Safety Rules (students)
- Staff Behaviour Policy
- Staff handbook
- Student Privacy Notice
- Data Protection Policy

**Useful links to external organisations:**

Ofsted
www.gov.uk/government/publications/school-inspection-handbook

DfE
www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

CEOP
www.ceop.police.uk/safetycentre/
www.childnet-int.org/

UK Safer Internet Centre
www.saferinternet.org.uk/safer-internet-day
www.saferinternet.org.uk

Internet Watch Foundation
www.iwf.org.uk
www.iwf.org.uk/members/get-involved

Links to training
CEOP: www.ceop.police.uk/training/
EPICT: offline and online online safety training: www.epict.co.uk/#!esafetyinfo/cq8q

**Movies and presentations**

www.swgfl.org.uk/products-services/online-safety/resources/SWGfL-E-Safety-Movies
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

**Other publications**

Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DSF and DCMS, 2008
http://webarchive.nationalarchives.gov.uk/20100407120701/dcsf.gov.uk/byronreview/

Ofcom's response to the Byron Review, Ofcom, 2008
http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/

**Review**

The Governing Body of Limpsfield Grange School adopted this policy on: _____

It will be reviewed on: _____
Signed _____
Dated _____