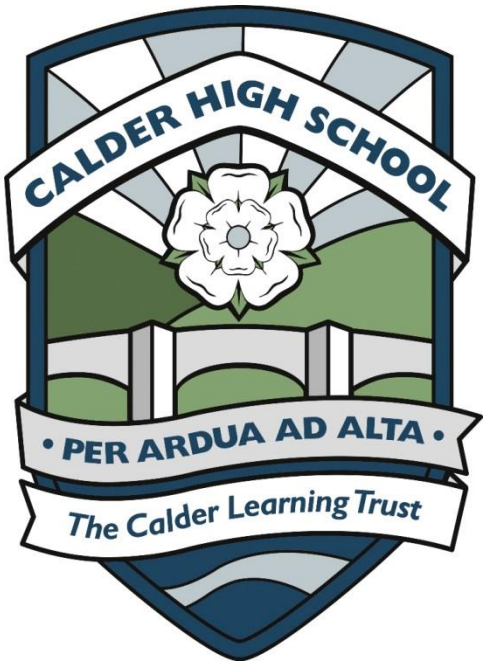

ACCEPTABLE USER POLICY

Acceptable User Policy: Calder High School

The acceptable use of the school network, Internet and related technologies

Contents

This e-Safety Policy has been written by Calder High School, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed annually.

Context

Harnessing Technology: Transforming learning and children's services[1] sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, e-Strategy 2005

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3], *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

---

[1] http://www.dfes.gov.uk/publications/e-strategy/

[2] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3] See Every Child Matters website [http://www.everychildmatters.gov.uk]

[4] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of Calder High School to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff, governors and the school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Acceptable User Policy: Calder High School

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http://www.facebook.com
- www.twitter.com HYPERLINK "http://www.snapchat.com/" www.snapchat.com)
- Dating sites (www.tinder.com HYPERLINK "http://www.match.com/" www.match.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ HYPERLINK "http://www-kazzaa.com/" http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for students, staff and parents.

Reference: Becta - e-Safety Developing whole-school policies to support effective practice[5]

3. Teaching and Learning

3.1 Why internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

3.2 Internet use will enhance and extend learning

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

---

http://schools.becta.org.uk/index.php?section=is [5] http://schools.becta.org.uk/index.php?section=is

3.3 Students will be taught how to evaluate Internet content

- Calder High School will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to two members of the Senior Leadership Team who also have responsibility for Child Protection.

Our school **e-Safety Co-ordinators** are Mr R Sutcliffe and Mr S Newton

Our e-Safety Co-ordinators ensure they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[6]. The school's e-Safety coordinators ensure the Headteacher; Senior Leadership Team and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance[7] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of student information/photographs and use of website;
- e-Bullying/Cyber bullying procedures;
- their role in providing e-Safety education for students;

Technical Staff will be responsible for the blocking of email, internet and network access following an infringement. They will inform the Headteacher and eSafety Co-ordinators of this action. They will liaise with the e-Safety Co-ordinators to investigate the infringement and the imposition of agreed sanctions.

Staff are reminded/updated about e-Safety matters at least once a year via Inset.

---

[6] http://www.ceop.gov.uk/

[7] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

4.1 Safe use of email.

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher or other member of staff if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

4.2 Safe use of Internet including use of internet-based communication services, such as instant messaging and social network.

- School will block access to social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students must not place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.

4.3 Safe use of school network.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Calder High School will work in partnership with Calderdale LA, Calderdale CLC, DCSF and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Co-ordinators or the Network Manager.
- All users are asked to respect the privacy of files of other users. Students are asked not to enter file areas of other users without obtaining permission first. All users are reminded that files to be shared should be saved to the shared areas available. Students have the facility to read the Curriculum Public drive but not write to it. Students should be reminded that they can share files via the Public drive through consultation with the Network Manager.
- All users accessing software or any services available through the school network must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. All users should be aware that some items are licensed for educational or restricted use only.

4.4 Safe use of passwords.

- All users are expected to be responsible for their own areas on the school network.
- Passwords are set for each user.
- Passwords should be a minimum of 6 characters and can contain numbers. They should not contain spaces
- Passwords should not be shared with other users.
- It is recommended that passwords are changed regularly.
- Users requiring assistance in changing their password should contact the Network Manager.

4.5 Safe use of equipment.

Students must treat with respect equipment in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Students should be reminded that any malicious action will result in the immediate suspension from use of the school facilities.

4.6 Protection of personal data.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4.7 Safe use of digital images and digital technologies, such as mobile phones and digital cameras.

- Photographs that include students will be selected carefully so that individuals cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Work can only be published with the permission of the student and parents/carers
- Parents/guardians are informed that photographs including images of students will be used on display boards, the school website and other promotional materials for the benefit of the school. Parents have the opportunity to request that images of their child are not used if they so wish.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones must be switched off whilst in school and are not allowed to be used unless;
    - Students are given express permission by a member of staff (usually the Headteacher or SLT).
    - It is break or Lunchtime and students are not inside the school

Students who choose to bring phones into school do so at their own risk. Calder High School is not responsible for the theft, loss or breakage of any valuable goods.

- Calder High School does not take any responsibility for them. Students using mobile phones in school to phone or text will have them confiscated and returned at 3pm. Excessive incidents of mobile phone use will result in confiscation for parents to collect from school.
- The use by students of digital cameras, mobile phones containing digital cameras is not permitted. Students may only access digital cameras via curriculum based activities and under the supervision of staff
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. They are not permitted in school or on any educational based activity.
- IPOD and MP3 players are not permitted in school. Students who choose to bring them into school do so at their own risk. Students using such items in school will have them confiscated and returned to them at the end of the school day.
- Staff will be issued with a school phone where contact with students is required.
- Staff are not permitted to take photos of students with their personal camera/camera phones

4.8 Publication of student information, photographs and use of website.

- Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Staff or student personal contact information will not be published i.e. addresses and personal telephone numbers. The contact details given online would normally be via the school office.
- Staff requesting to use images of students who are looked after by the Local Authority should seek permission from the Social Worker before publishing any images.
- Parents are informed that photographs including images of students will be used on display boards the school website and other promotional materials for the benefit of the school. Parents have the opportunity to request that images of their child are not used if they so wish.
- The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

4.9 e-Bullying and Cyber bullying procedures.

Cyber bullying can be defined as abusive or threatening behaviour via text messaging, e-mail, chat rooms, discussion boards, social networking sites and instant messaging services. Also 'bluejacking' where anonymous text messages are sent short distances using wireless 'bluetooth' technology.

Students must be made aware that this behaviour will not be tolerated and also that sending abusive or threatening messages is against the law. It is also against the law to forward abusive texts, e-mails, messages or images.

e-Bullying and Cyber bullying will be treated in line with Calder High School's Anti-Bullying policy. Students who are being bullied by email, text or online should keep and save any bullying emails, text messages or images, and note times and dates of messages and details about the sender.

Staff and students should refer to the DSL – Mr Taylor or Safeguarding Officer – Mrs Baxter. The incident will then be investigated in line with the Anti-Bullying policy and if appropriate report to the Child Protection Governor.

4.10 Curriculum role in providing e-safety education for students.

All students will be given e-Safety lessons at the start of each academic year as part of the ICT/L4L curriculum schemes of work and awareness through SMSC in Assemblies.

Acceptable User Policy: Calder High School

5. Policy Decisions

5.1 Authorising Internet access.

- All staff must read and sign the Acceptable Users Policy (see appendix 1.1) before using any school ICT resource.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the responsible Internet Use statement (see appendix 1.2).
- Parents/carers will be asked to sign and return a consent form.

5.2 Assessing risks.

Calder High School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Calderdale LA can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective. This will take place on an annual basis

5.3 Handling e-Safety complaints.

- Complaints of Internet misuse will be dealt with by the e-Safety Co-ordinators.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents/guardians will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

5.4 Community use of the Internet.

The school will liaise with local organisations to establish a common approach to e-Safety.

Acceptable User Policy: Calder High School

6. Communicating e-Safety

6.1 Introducing the e-Safety policy to Students.

- e-Safety rules will be posted in all rooms where computers are used (see appendix 1.3)
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed, and delivered at the start of each academic year.

6.2 Staff and the e-Safety policy.

- The Policy is part of the Staff Handbook which should be reviewed annually by staff and used as part of the induction of new staff.
- Staffare informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with Students can lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff should refer to the document "Guidance for Safe Working Practice for the Protection of Children and Staff in Education Settings": Communication with children and adults, by whatever method, should take place within professional boundaries and staff should avoid any personal subject matter. This includes the wider use of technology such as mobile 'phones, text messaging, e-mails, digital cameras, videos, web-cams, websites, social network sites and blogs.
- Staff accept all the conditions above when logging on the every school computer.

6.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- The school will maintain a list of e-Safety resources for parents/carers which is available on the parental page of the school website.

7. Infringements and Sanctions

Any failure to comply with the Acceptable User Policies may lead to temporary or permanent suspension of the use of ICT facilities. The Headteacher, within their discretion, may waive or vary a penalty if the circumstances warrant such action.

7.1 Student infringements and Sanctions

Where a student fails to adhere to the responsible user's agreement, sanctions will be imposed. The final level of the sanction will be at the discretion of the Senior Leadership Team via discussion with the appropriate Curriculum Manager and the school Network Manager.

Category A infringements:

- Use of non educational sites during lessons.
- Unauthorised use of school email system.
- Use of unauthorised instant messaging system.

Sanction: Referral to Class Teacher and/or Curriculum Manager. Loss of internet and email access for a fixed period.

Category B infringements:

- Continued use of non educational sites during lessons after receiving a warning.
- Continued unauthorised use of school email system after being warned.
- Continued unauthorised use of instant messaging system.

Sanction: Referral to Curriculum Manager/Line Manager of Department. Loss of internet and email access for set period of time. Contact with home regarding incident and sanctions imposed.

Category C infringements:

- Physical damage to school equipment.
- Deliberately trying to access inappropriate and offensive internet sites.
- Sending inappropriate and offensive emails.
- Corrupting data belonging to another individual.
- Attempting to purchase or order items over the Internet.

Any other inappropriate use or abuse of the school network and internet systems that contravene the agreed responsible user policy.

Sanction: Referral to SLT for final sanction to be imposed.

In every category internet and email access will be suspended with immediate effect whilst an investigation of the incident takes place.

For more serious offences such as Category C offences, a ban of access to the network system will be imposed while the offence(s) is investigated. A sanction will then be imposed.

7.2 Staff infringements and Sanctions

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online
- shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on school network.

Sanction: Referral to Line Manage and managed through the Discipline Policy.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to any school computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing and downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988.
- Bringing the school name into disrepute.
- Inappropriate communications with students and minors under the age of 18.

Sanction: Referral to Headteacher and Governors.Managed through the Discipline Policy.

Other safe guarding actions:

- Removal of staff PC/ Laptop to a secure place to ensure that there is no further access to the PC/ Laptop.
- Instigate an audit of all ICT equipment by an outside agency, to ensure there is no risk of students accessing inappropriate materials in school.
- Identify the precise details of the materials.

If a member of staff commits an exceptionally serious act of gross misconduct they will be instantly suspended. There would normally be an investigation before disciplinary action is taken for an alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before the disciplinary action is taken.

Calder High School will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

In the case of Child Pornography being found, the member of staff will be immediately suspended and the Police will be called. Be aware that anyone can report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): www.ceop.gov.uk/reporting.abuse.html

7.3 Informing Staff and Students of procedures

- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so that they develop 'safe behaviours'.
- Staff and Students will be required to sign the acceptable user policy.
- Staff will be made aware of the infringements and sanctions via Inset training and the staff handbook. The e-Safety policy will be available via the staff shared area.
- Students will be made aware of the infringements and sanctions via curriculum and posters made available in networked areas.
- The school e-Safety policy will be made available to all users, parents/guardians via Calder High School website.

Appendix

Acceptable User Policy: Calder High School

Student Acceptable Use Policy / e-Safety Rules

ICT and the related technologies such as the internet and email are an important part of learning in our school.

We expect all Students to be responsible for their behaviour when using ICT and the Internet. It is essential that Students are aware of e-Safety and know how to stay safe when using any ICT.

Students are expected to discuss this policy with their parent or guardian and then to sign and follow the e-Safety Rules. Any concerns or explanation can be discussed with their class teacher or the e-Safety coordinator.

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school's AUP relates to Computer Use and Internet Access and has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files or emails that may be held on its computer systems or to monitor any Internet sites visited.

- Access must only be made via the authorised account and password, which must not be made available to any other person.
- You must not gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data.
- All Internet use should be appropriate to staff professional activity or student's education.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received.
- The normal rules of social interaction apply to e-mail. The remoteness of the recipients must not be used to excuse anti social behaviour, harassment, intimidation and bullying behaviour.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages, use of chat rooms and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Legitimate private interests may be followed, providing school use is not compromised.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- You must check your email daily as this is how staff will communicate important information to you.

Students in breach of these regulations may find their access withdrawn and persistent misuse of the network could lead to an exclusion from school.

Parent and Student signatures

We have discussed this policy and ……..(Student name) agrees to follow the e-Safety Rules and to support the safe use of ICT at School.

Parent/ Carer Signature ……

Student Signature ……

Form …… Date ……

Appendix 1.1

Acceptable User Policy: Calder High School

Staff Acceptable Use Policy / Code of conduct

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-Safety coordinator.

Failure to follow this policy may result in disciplinary action in accordance with the school's e-safety policy.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given
- I will not access other network user's files unless specifically authorized to do so
- I will ensure that all electronic communications with Students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to Students or colleagues material that could be considered offensive or illegal
- Images of Students will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help Students to be safe and responsible in their use of ICT and related technologies.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only use LA systems in accordance with any Corporate policies.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school. I have read and understood the e-Safety Policy.

Signature ……

Date ……

Full Name …… (printed)

Job title . . . . . .

Appendix 1.2

14

Responsible ICT System and Internet Use – Sanctions - Students

Where a student fails to adhere to the responsible user's policy, sanctions will be imposed. The final level of the sanction will be at the discretion of the Senior Leadership Team via discussion with the Curriculum Manager for ICT and the school Network Manager.

Category A infringements:

- Use of non educational sites during lessons.
- Unauthorised use of school email system.
- Use of unauthorised instant messaging system.

Sanction: Referral to Class Teacher and / or Curriculum Manager of ICT, loss of Internet and email access for a fixed period.

Category B infringements:

- Continued use of non educational sites during lessons after receiving a warning.
- Continued unauthorised use of school email system after being warned.
- Continued unauthorised use of instant messaging system.

Sanction: Referral to Curriculum Manager of ICT/Line Manager of ICT Department, loss of Internet and email access for set period of time. Contact with home regarding incident and sanctions imposed.

Category C infringements:

- Physical damage to school equipment
- Deliberately trying to access inappropriate and offensive Internet sites
- Sending inappropriate and offensive emails.
- Corrupting data belonging to another individual.
- Attempting to purchase or order items over the Internet.

And any other inappropriate use or abuse of the school network and Internet systems that contravene the agreed responsible user policy.

Sanction: Referral to SLT for final sanction to be imposed

In every category Internet and email access will be suspended with immediate effect whilst an investigation of the incident takes place. A sanction will then be imposed.

Appendix 1.3

Acceptable User Policy: Calder High School

Responsible ICT System and Internet Use – Sanctions - Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online
- Shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on school network.

Sanction: Referral to Line Manager. Headteacher Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to any school computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing and downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988.
- Bringing the school name into disrepute.

Sanction: Referral to Headteacher and Governors. School disciplinary procedures followed.

Other safe guarding actions:

- Removal of staff PC/ Laptop to a secure place to ensure that there is no further access to the PC/ Laptop.
- Instigate an audit of all ICT equipment by an outside agency, to ensure there is no risk of students accessing inappropriate materials in school.
- Identify the precise details of the materials.

If a member of staff commits an exceptionally serious act of gross misconduct they will be instantly suspended. There would normally be an investigation before disciplinary action is taken for an alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before the disciplinary action is taken.

Calder High School will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

In the case of Child Pornography being found, the member of staff will be immediately suspended and the Police will be called. Be aware that anyone can report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): www.ceop.gov.uk/reporting.abuse.html

Appendix 1.4

Calder High School

e-Safety Co-ordinators:

Mr A Taylor – Deputy Head

Mr R Sutcliffe – Network & Systems Manager, CEOP

Mrs N Baxter – Safeguarding Manager

Guidance: What to do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child

1. Play the situation down: don't make a drama.
2. Report to the headteacher/e-Safety co-ordinator who will decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered.

An inappropriate website is accessed <u>intentionally</u> by a child

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents/guardian of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the headteacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal.
   The headteacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of ICFT equipment by the school's ICT Network Manager to ensure there is no risk of Students accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature the headteacher should then:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - Inform Personnel/Human Resources.
   - If requested, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time

- Inform the School e-Safety co-ordinator.
- Advise the child not to respond to the message.

The e-Safety co-ordinator will then:

- Refer to relevant policies including e-Safety, anti-bullying and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's email service provider.
- Notify parents of the children involved.
- Inform the police if necessary.

Appendix 1.5 (1)

Malicious or threatening comments are posted on an Internet site about a Student or member of staff

If the comments have come from an external source.
Report the incident to the e-Safety co-ordinator who will:

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform the police as appropriate.
5. Inform the LA e-Safety co-ordinator.

If the comments have come from an internal

source: 1. Refer to e-Safety co-ordinator for

investigation. The e-Safety co-ordinator will then:

a) Refer to acceptable user policy that was signed by the child, and apply agreed sanctions.
b) Notify parents of the child responsible/child affected by comments.
c) Inform the school technician and ensure all evidence is secure and preserved.
d) Consider the involvement of the police.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with a child

1. Report to and discuss with the named child protection officer/e-Safety co-ordinator.

The e-Safety co-ordinator will then:

a) Advise the child on how to terminate the communication and save all evidence.
b) Contact CEOP http://www.ceop.gov.uk/
c) Consider the involvement of police and social services.
d) Inform the LA e-Safety Co-ordinator.

All of the above incidents must be reported immediately to the headteacher and e-Safety co-officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Acceptable User Policy: Calder High School

Calder High School Network Account Request Form

Student request form

(For students to fill in)

Please fill in the details below and pass to IT Support for processing

Surname ..... (BLOCK CAPITALS)

First Name ..... (BLOCK CAPITALS)

Second name or initial ..... (BLOCK CAPITALS)

Form ..... (BLOCK CAPITALS)

As a school user of the Internet, I agree to comply with the rules on its use.
I will use the school network in a responsible way and observe all the restrictions explained to me by the school.
I confirm that I have read and understand the Student Acceptable Use Policy / e-safety rules.

Student Signature……..

Date: ___ / ___ / ___

▪ _____

(For IT Support Staff to fill in)

Below please find your newly created logon details

Account User Name…….

Initial password……(you will be required to change this on your first logon)

Date created……../……/…….

Created by…….

Appendix 1.6

Calder High School Network Account Request Form

Staff request form

(For staff to fill in)

Please fill in the details below and pass to IT Support for processing

Surname ..... (BLOCK CAPITALS)

First Name ..... (BLOCK CAPITALS)

Second name or initial ..... (BLOCK CAPITALS)

Position (Teacher / Support Staff etc) ..... (BLOCK CAPITALS)

Serco Access required? (Yes / No) ..... (BLOCK CAPITALS)

As a school user of the Internet, I agree to comply with the rules on its use.
I will use the school network in a responsible way and observe all the restrictions explained to me by the school.
I confirm that I have read and understand the Staff Acceptable Use Policy / Code of Conduct.

Staff Signature.....

Date: ___ / ___ / ___

·_____

(For IT Support Staff to fill in)

Below please find your newly created logon details

Account User Name.....

Initial password.....(you will be required to change this on your first logon)

Serco Log on details (if applicable)

Serco Username.....

Serco Password.....

Date created...../...../.....

Created by.....

Acceptable User Policy: Calder High School

Authorised Signature (Head teacher)

Is this member of staff temporary? NO / YES If yes, contract end date: ……

I approve this email account / connection to the Internet / Intranet.

Signature ……..…….. Date ……

Full Name …… (printed)

We recommend: One copy is retained by member of staff | Second copy for school file

Appendix 1.7