Drumbeat
School & ASD Service

Online Safety Policy

Updated: Reviewed July 2023

Responsible Person	Charlotte Finch
Signed by Chair of Governors	MGabriel
Signed by Executive Headteacher	Marie Neave
Date approved	July 2023
Review date	July 2024

The acceptable use of the internet and related technologies

Online Safety Policy Overview

This document should not be read in isolation and should has direct links to the following school policies;

- Social Networking Policy.
- Safeguarding Policy.
- Anti-bullying Policy.

ICT at Drumbeat

The extent to which information and communication technology (ICT) capability and other key skills improve the quality of pupil's learning and progress.

The extent to which learners adopt safe and responsible practices in using new technologies, including the Internet.

The extent to which pupils develop workplace and other skills that will contribute to their future economic well-being.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

Drumbeat strives to ensure that children and young people are:

- 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 messaging; 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 the school to ensure that every child in their 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 and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. 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 often using simple web cams or mobile phones.
- Podcasting
- Social networking sites (Sites such as Facebook, WhatsApp and SnapChat
- Video broadcasting sites (Sites such as YouTube and Instagram)
- Chat Rooms (Sites such as Kidschat, 321chat, talkwithstranger, chatogo, Kidsworld
- Gaming Sites (Sites such as Neopets, Runescape, Worldofwarcraft and ClubPenguin
- Music download sites (sites such as Amazon, iTunes, Napster, and google play
- Mobile phones with internet, camera and video functionality
- Mobile technology (e.g. games consoles) that link to the internet

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;
- An e-Safety education programme for pupils, staff and parents.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Executive Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Executive Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **E-Safety Co-ordinator** is Katie Denton.

Our e-Safety Coordinator ensures 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 LGfL and NSPCC

Exploitation and Online Protection (CEOP) http://www.ceop.gov.uk/. The school's e-Safety coordinator ensures the SLT 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 on e-Safety and are updated regularly 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 pupils 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 networks;
- 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 pupil information/photographs and use of the website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

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

Schools should include e-safety in the curriculum and ensure that every pupil has received guidance about safe and responsible use appropriate to their needs and level of usage. Pupils need to know how to control and minimise online risks and how to report a problem. Schools should ensure that they make efforts to engage with parents over e-safety matters.

Communications

Pupils

Pupils' perceptions of the risks may not be mature; the e-safety rules may need to be explained or discussed. Useful e-safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- The BBC's ChatGuide
- E-safety will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

Staff

Staff should feel confident to use ICT in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, premises, governors and volunteers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Internet use in pupils' homes is increasing. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Through a partnership approach the school may be able to help parents plan appropriate supervised use of the Internet at home.

How will complaints regarding e-safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher / e-Safety Coordinator / Executive Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Executive Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time ‘remote’ training support;
- secure data exchange between local and government bodies.

The Risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

Technology and Infrastructure Drumbeat School:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students; for example most classes access some educational content through Youtube and this has age appropriate restrictions in place.
- Ensures network healthy through use of anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files; set by IT facilities support (SNS)
- Uses individual, audited log-ins for all users - the London USO system; set by IT facilities support (SNS)
- Uses DfE, LA or LGfL approved systems such as S2S, Egress or USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site; set by IT facilities support (SNS)
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons; set by IT facilities support (SNS) on the request of the school.
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network and Itunes
- Uses mail for students as set by set by IT facilities support (SNS).
- Provides staff with an email account for their professional use through London Staffmail and makes clear personal email should be through a separate account;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

Policy and Procedures: Drumbeat School

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within the appropriately secure school's learning environment, such as the school website.
- Requires staff to preview websites before use.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google safe search, yahoo for kids or ask for kids
- Is vigilant when conducting 'raw' image search with pupils e.g. Google;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary via SNS;
- Requires pupils to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named safeguarding officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides Esafety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and Training Drumbeat School

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages appropriate to the children and young people's abilities, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age, ability and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;

    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes training available to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - distribution of 'think u know' for parents materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Managing Email

E-mail is now an essential means of communication for staff in schools and everyday life. Directed use of regulated e-mail in schools can bring significant educational benefits, increases the ease of communication with parents and within the school community and facilitates local and international school projects. However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate. In the school context, e-mail should not be considered private and Drumbeat school reserves the right to monitor e-mail.

Drumbeat School:

- Does not publish personal e-mail addresses of pupils on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively with up to date account details of users.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff should only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, CyberDuck;
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Use of Digital and Video Image

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff oversees /authorises the website's content and check suitability.

Use of still and moving images

Care is taken when using photographs or video footage of pupils on the school website. The first and last name will not be used with a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- **If the pupil is named, avoid using their photograph / video footage. If the photograph /video is used, avoid naming the pupil.**
- If the school website is using a webcam – then this will be checked and monitored to ensure misuse does not occur accidentally or otherwise.

Technical:

- Digital images / video of pupils will be stored securely on the school network and old images deleted after a reasonable period.

Education:

- Staff should report any inappropriate use of images to a member of the senior leadership team and understand the importance of safe practice. Pupils should be encouraged to report such images to staff. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

At Drumbeat School:

- The Executive Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the Head teacher, Deputy Headteacher, School Business Director and the Headteachers's PA.
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

Managing Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network 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 reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely Drumbeat school:

- Will ensure staff read and sign that they have understood the school's e-safety Policy.
- Provides pupils as appropriate with an individual e-mail log on;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;

- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed including PAT testing and cleaning of projector filters.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems for technical support for IT technical support; SIMs; Visitor Access system and Smart Diary support.
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. In the case of students infringing the policy parents will always be contacted within all categories in order to support and signpost e-safety at home and links to safeguarding.

The following are provided as examples only:

Students

Category A infringements:

- Use of inappropriate internet sites
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in school
- Use of unauthorised instant messaging / social networking sites

If the infringement has been knowingly committed the matter will be investigated by the class teacher

Category B infringements:

Where a pupil or young person knowingly:

- Continues use of inappropriate sites after being warned
- Continues unauthorised use of email after being warned
- Continues unauthorised use of mobile phone (or other new technologies) after being warned

- Continues use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Corrupts or destroys others' data without notifying a member of staff.
- Accesses offensive material and does not log off or notify a member of staff of it

Such incidents would be referred to the Assistant Headteacher and internet access/ mobile device will be removed for an appropriate period.

Category C infringements:

- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Such incidents would be referred to the E-safety co-ordinator or Head Teacher and parents may be contacted.

Other safeguarding actions:

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / LGFL as appropriate

Category D infringements:

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, 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

Such incident would be referred to the Executive Headteacher and Parents would be contacted. The Community Police Officer may be involved.
Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender’s e-mail service provider

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.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff members professional standing in the school and community including inappropriate use of social networking sites

- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Sanction - **referred to line manager / Headteacher**. Warning given.

Category B infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, 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 – **Referred to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

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

Schools are likely to 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.

Child sexual abuse images found?

In the case of child sexual abuse images being found, the member of staff should be **immediately suspended** and the Police should be contacted: free phone: **0808 100 0040** DSL will contact the LA.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reportingabuse.html
http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Where appropriate Pupils will sign an age appropriate e-safety / acceptable use form;

- The school’s e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.
- Staff are issued with the ‘What to do if?’ guide on e-safety issues.

Parents E-Safety Agreement Form

Parent / guardian name: ________________ ______________________________

Pupil name(s): ____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, London Grid for Learning (LGfL) e-mail and other ICT facilities at school.

I know that where appropriate my daughter or son has signed an e-safety agreement form and been shown the 12 ‘rules for responsible ICT use’.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child’s computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

Parent / guardian signature:_______________________ Date: _____/_____/_____

E-Safety Form for Pupils'

Think before you click

I will only use the internet and email with an adult

I will only click on icons and links when I know they are safe

I will only send friendly and polite messages

If I see something I don't like on a screen, I will always tell and adult

My Name:

My Signature:

Staff Agreement Form - Acceptable Usage Policy (AUP)

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal any personal password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business which is currently staff mail unless approved by the Head Teacher or School Business Manager.
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / e safety co-ordinator.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- If applicable, I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role, and will not in any way bring the school or colleagues into disrepute by inappropriate postings on social networking sites.
- 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 ensure that any equipment taken out of school on loan other than during school visits will be my responsibility and should loss/damage occur liability will be covered by personal insurances.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.

- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and e-mails can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I agree to abide by all the points above.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ______________________________ Date ________________

Full Name ______________________________ (printed)

Job Title ______________________________

School ______________________________

Authorised Signature (Deputy Head Teacher/School Business Director)

I approve this user to be set-up.

Signature ______________________________ Date ________________

Full Name ______________________________ (printed)

Safeguarding and Protecting Children Guidance

What are the e-safety issues?

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the wellbeing of children may also exist in a variety of other ways.

It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with.

This process is known as ‘Grooming’ whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.

An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

Section 175 of the 2002 Education Act and Section 11 of the 2004 Children Act places upon all those who work with children a duty to safeguard and promote their welfare by creating a safe learning environment and where there are child welfare concerns, taking swift action to address them. It is vital that schools are aware of the signs which might indicate that a child is being groomed, bullied or being subjected to inappropriate material and know how to take steps to begin to address this and safeguard and support the child.

Creating a safe learning environment means having effective arrangements in place to address a range of issues and schools should ensure that they have policies and procedures in place which are reviewed annually and adhered to by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

Cyberbullying Guidance

Key national document:

Cyberbullying – Safe to Learn: Embedding Antibullying work in schools” DCSF-00658-2007

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (e.g. MySpace) or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail (such as ‘Happy Slapping’ videos)

It should be noted that the use of ICT to bully could be against the law.

Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984* for example.

Bullying is when someone deliberately hurts you or makes you unhappy. It will be repeated and be difficult to defend yourself against it. Bullying can be racist, sexist or homophobic.

Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the bullied emotionally and/or physically.

The following will be appended to our **Anti-bullying Policy**

Drumbeat School will not tolerate the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff.

We consider that bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender's e-mail service provider
5. Notify parents of the children involved
6. Consider informing the police depending on the severity or repetitious nature of offence
7. Inform the e-safety co-ordinator.

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

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 e-safety co-ordinator.*
4. *Endeavour to trace the origin and inform police as appropriate*

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. "

Guidance - What do we 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 it into a drama.
2. Report to the head teacher/e- safety officer and 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 of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an Lgfl.

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 head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
    a. Remove the PC to a secure place.
    b. Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    c. Identify the precise details of the material.
    d. Take appropriate disciplinary action (contact Personnel/Human Resources).
    e. Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
    a. Contact the local police or High Tech Crime Unit and follow their advice.
    b. If requested to 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:

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

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

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Endeavour to trace the origin and inform police as appropriate.
4. Inform e-safety co-ordinator.

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 the child:

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.

3. Consider the involvement police and social services.
4. Inform LA safeguarding officer.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

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

12 Rules for responsible ICT use

Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others:

- I will only use the school’s computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people’s files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.