E-Safety & Data Protection Policy

E-Safety Officers: Martin Lubich and Lucy Tierney

Date: February 2016

Policy Review Date: 2019

Contents

Acknowledgements:

London Grid for Learning | South West Grid for Learning

Overview

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Children and young people have an entitlement to safe internet access at all times.

The requirement to ensure that pupils are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. The dangers they may face include:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

(from Inspecting E-Safety, Ofsted Sept 2012 available at www.ofsted.gov.uk/resources/120196)

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This policy explains how we intend to do this, while also addressing wider educational issues in order to help pupils (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Roles and Responsibilities

This section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

Governors: The Governing Body are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

Headteacher: The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team are responsible for:

- Ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- Ensuring there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role.
- Ensuring they receive regular monitoring reports from the E-Safety Co-ordinator.

The Headteacher and another member of the Senior Leadership Team should be aware of the Local Authority procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

The E-Safety Team:

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
- Attends relevant meetings / committee of the Governing Body
- Reports regularly to Senior Leadership Team

Technical Support Staff/ Agencies: It is the responsibility of the school to ensure their technical support company and technicians carry out any E-Safety measures, and that they are aware of this policy. Their role might include:

- Ensuring the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring the school meets the E-Safety technical requirements outlined by the LGfL and Local Authority guidance

- Ensuring users may only access the school's networks through a properly enforced password protection policy
- Ensuring the LGfL is informed of issues relating to the filtering applied by the Grid

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)(Appendix 3)
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation, action or sanction
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school E-Safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that they follow the procedure in place for dealing with any unsuitable material that is found in internet searches

The Designated Child Protection Officer: is aware of the potential for serious child protection issues that may arise arise from:

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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (Appendix 2), which they will be expected to sign before being given access to school systems**.**
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

- Understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers: Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local E-Safety campaigns. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy if appropriate
- Endorsing (by signature) the Permissions Letter regarding their child's use of the internet and use of their child's images (Appendix 1)
- Accessing the school website, MLE, and any on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users: Any users who access school ICT systems as part of the Extended School provision will be expected to sign an Acceptable Use Policy before being provided with access to school systems. (Appendix 3)

Managing the Internet Safely

Infrastructure and technical

This school:

- Has 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
- Ensures the network remains healthy through the use of Sophos anti-virus software (from LGfL) and network set-up so staff and pupils cannot download executable files
- Uses individual, audited log-ins for all users - the London USO system
- Uses DfE, LA or LGfL approved systems such as S2S, 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
- 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

- Only uses the LGfL / NEN service for video conferencing activities
- Uses security time-outs on Internet access where practicable / useful
- If email is used with pupils, we use Londonmail as this has email content control and the address does not identify the student or school
- Provides staff with an email account for their professional use (*London Staffmail)*, and makes clear personal email should be through a separate account
- Uses a 'remote' management control tool (the Ranger Management System) for controlling workstations / viewing users / Internet web sites, when appropriate
- 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 Technical Support Provider is up-to-date with LGfL services and policies

Policy and procedures

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in areas where older pupils have more flexible access
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age or subject appropriate web sites
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where appropriate; eg yahoo for kids or ask for kids
- Is vigilant when conducting 'raw' image or internet searches with pupils e.g. Google image search
- 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 E-Safety Team. Our administrator logs or escalates as appropriate to LGfL or Atomwide as necessary
- Requires pupils to individually sign an Acceptable Use Form which is fully explained and used as part of the teaching programme (Appendix 2)
- Requires all staff to sign an Acceptable Use Form, and keeps a copy on file (Appendix 3)
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the Permissions agreement form at time of their child's entry to the school (Appendix 1)

- Makes clear all users know and understand what the rules of appropriate use are, and what sanctions result from misuse – through staff meetings and in lessons for pupils
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system (Appendix 4)
- Ensures the named child protection officer has appropriate training
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides E-Safety advice for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities, e.g. the Police and/or the LA.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher or 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 their monitor and report it to the teacher / supporting adult
- Ensures pupils and staff know what to do if there is a cyber-bullying incident (Appendix 4)
- Ensures all pupils know how to report any abuse
- Has a clear E-Safety education programme throughout all Key Stages, built on Local Authority, LGfL and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age 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 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, 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
    - 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, and 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. For example, risks in pop-ups, buying things online

- 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

- Runs a rolling programme of advice, guidance and training for parents, including:

    - Information leaflets, in school newsletters and on the school web site
    - meetings held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents

Use of digital and video images

In this school

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school

- Digital images /videos of pupils are stored in a private 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 identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials

- 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 (Appendix 3)

- The school blocks access to social networking sites or newsgroups unless there is a specific approved educational purpose

- Pupils are taught about how images can be manipulated in their E-Safety education programme and are also taught to consider how to publish for a wide range of audiences

which might include governors, parents or younger children as part of their ICT scheme of work

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

School Trips

On school trips, NO pupils should carry their own mobile phones or take photographs using their phones. The lead teachers will have mobile phones to use in the case of an emergency, and will also carry digital cameras for taking photos.

Parents accompanying classes on trips may take their own mobile phones and take photographs, but must be made aware that these images are for their private family use only and must not be shared on the Internet in any form e.g. via Facebook, as stated in the Parent Permission Forms (Appendix 1)

Website

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website administrators
- 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, telephone number and we use a general email contact address: admin@edenprimary.org.uk. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website

Learning Platform (Fronter MLE)

- Uploading of information on the schools' Managed Learning Environment (MLE) is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the schools MLE will only be accessible by members of the school community
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' Learning Platform for such communications

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

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.

Personal Devices

Staff are allowed to bring personal devices such as mobile phones, iPads etc. into school but must follow the rules set out in the Staff and Volunteer Acceptable Use Agreement. (Appendix 3)
Pupils should not have mobile phones or other personal devices in school. If any such devices are brought in they should be handed into the office for safe-keeping at the beginning of the day, and collected at home time.

On school trips, NO pupil should carry their own mobile phones or take photographs using their phones. The lead teachers will have mobile phones to use in the case of an emergency, and will also carry digital cameras for taking photos.

Parents accompanying classes on trips may take their own mobile phones and take photographs, but must be made aware that these images are for their private family use only and must not be shared on the Internet in any form e.g. via Facebook, as stated in the Parent Permission Forms (Appendix 1)

Policy and procedure

This school:

- Ensures staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with email and network access. Access is through a unique username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes
- All pupils have their own unique username and password which gives them access to the Learning Platform and/or Purple Mash
- In KS2 we use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as 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
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- 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.
- Has set-up the network so that specified users cannot download executable files / programmes
- 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[1] (Appendix 7)

[1] "'Use for private purposes' means any use that is not use in performing the duties of the employee's employment." HMRC EIM21613 Section 316(2) and (3) ITEPA 2003

- Maintains equipment to ensure Health and Safety is followed, for example our projector filters are cleaned by the site manager ; equipment is installed and checked by approved Suppliers
- 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, for example the SEN Co-ordinator to access SEN data
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved 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; e.g. technical support or MIS Support or our Education Welfare Officers accessing attendance data on specific children
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password)
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
- Uses the DfE 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 or through USO secure file exchange (USO FX)
- 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
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school ICT systems regularly with regard to health and safety and security

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 / LGfL 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 Local Authority if appropriate

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:
    - Remove the PC to a secure place.
    - 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.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).
    - Inform governors of the incident.

In an extreme case where the material is of an illegal nature:

- Contact the local police or High Tech Crime Unit and follow their advice.
- 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. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA E-Safety officer.

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. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA E-Safety officer.
6. Consider delivering a parent workshop for the school community.

We foster a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material or situation that makes them feel uncomfortable.

Infringements

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 and will reflect the school's behaviour and disciplinary procedures.

How will staff and pupils be informed of these procedures?

- All staff are required to read and sign the school's E-Safety acceptable use agreement form (Appendix 3)
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate acceptable use form (Appendix 2)
- 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 (Appendix 1)
- 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 (page 15)

Pupils:

Category A infringements	**Possible Sanctions:**
Use of non-educational sites during lessons Unauthorised use of email Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / E-Safety Coordinator
Category B infringements	**Possible Sanctions:**
Continued use of non-educational sites during lessons after being warned Continued unauthorised use of email after being warned Continued unauthorised use of mobile phone (or other new technologies) after being warned Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc Trying to buy items over online Accidentally corrupting or destroying others' data without notifying a member of staff of it Accidentally accessing offensive material and not logging off or notifying a member of staff of it	**Refer to Class teacher/ Head of Department / Year tutor / E-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]
Category C infringements	**Possible Sanctions:**
Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) Trying to access offensive or pornographic material (one-off) Purchasing or ordering of items online Transmission of commercial or advertising material	**Refer to Class teacher / Year Tutor / E-Safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions** **if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**

Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned Deliberately creating accessing, downloading or 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	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

Staff:

Category A infringements (Misconduct)	**Possible Sanctions:**
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. Misuse of first level data security, e.g. wrongful use of passwords. Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
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 creating ,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;	**Referred to Head teacher / Governors;** **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.

Bringing the school name into disrepute	Identify the precise details of the material. *Escalate to:* Report to LA /LSCB, Personnel Report to Police / CEOP where child abuse or illegal activity is suspected.

Data Protection

This school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Privacy Notice to all pupils/parents which summarises the information held on pupils, why it is held and the other parties to whom it may be passed on. (Appendix 5)

We ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- needs to have access to that data.

What is personal data?

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances[2]. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents/carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data eg class lists, pupil progress records or reports
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

General

[2] School Personal Data Handling Policy, SWGfL 2012

This school:

- Informs individuals why the information is being collected when it is collected
- Informs individuals when their information is shared, and why and with whom it was shared
- Checks the quality and the accuracy of the information it holds
- Ensures that information is not retained for longer than is necessary
- Ensures that when obsolete information is destroyed that it is done so appropriately and securely
- Ensures that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Shares information with others only when it is legally appropriate to do so
- Sets out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensures our staff are aware of and understand our policies and procedures

Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings, briefings and Inset

Secure storage of and access to data

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- All users with high level access (eg. Atomwide Nominated Contacts) will use strong passwords which must be changed regularly. User passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation
- Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected and/or encrypted
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection)
- the data must be securely deleted from the device once it has been transferred or its use is complete

The school has clear procedures for the backing up, accessing and restoring all data held on school systems, including off-site backups

All paper based Protected and Restricted (or higher) material must be held in lockable storage

Secure Transfer of Data and Access out of School

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;

- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event (nb. to carry encrypted material is illegal in some countries)

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance

with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging

The activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy

Reporting

All significant data protection incidents must be reported through the Senior Information Risk Officer (SIRO) to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).