Elstree School

Including all of the Pre-Prep Department and Early Years Foundation Stage

E-Safety Policy

Contents

Person responsible for Policy: **Head of ICT** Responsible Governor: **Gavin Owston**

Date of last revision: September 2019

Date to be revised: September 2021

1. Aims

- To protect staff
- To protect pupils
- To prevent staff from accessing inappropriate or unacceptable material
- To ensure appropriate use of the School's IT resources
- To ensure appropriate use of internet resources and services

2. Purpose

Current regulations hold employers liable for acts undertaken by their employees in the course of their employment and for the use of the employer's equipment and facilities outside the employee's normal employment.

The electronic computing and communications equipment and facilities installed at, or provided by Elstree School are specifically for the conduct of official school business. When and if these are used for personal or private purposes, the same standards of propriety are to be maintained. Infringements by staff of this Policy may lead to disciplinary proceedings or, in serious cases, instant dismissal.

Whilst recognising the benefits of these media for new opportunities for communication, this policy sets out the guidelines that staff of Elstree School are expected to follow when using social media.

It is crucial that pupils, parents and the public at large have confidence in the school's decisions and services. The principles set out in the policy are designed to ensure that staff uses social media responsibly so that confidentiality of pupils and other staff together with the reputation of the school are safeguarded.

All staff must be conscious at all times of the need to keep their personal and professional lives separate.

All staff are required to sign an Acceptable Use Policy for ICT or Code of Conduct for the use of the school's IT Services.

This policy should be read in conjunction with the following school policies and documents:

- Data Protection Policy
- Safeguarding and Prevent Policy
- Contract of Employment.
- E-Safety Policy

3. Staff responsibilities

This policy applies to Elstree School, the governing body, all teaching and support staff, whether employed directly by the school, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy.

Elstree School computing resources are provided for educational, training, or research purposes. School computing or network resources must not be used for any commercial or significant personal purposes, except subject to this policy and where specifically authorised. Software and/or information provided by the School may only be used for educational purposes unless explicitly informed to the contrary. Staff members agree to abide by all the licensing agreements for software entered into by the School with other

parties.

As part of the beginning of term inset programmes, staff are trained in safeguarding procedures which includes staying safe online. Visiting speakers include Karl Hopwood from 'e Safety Ltd' (Summer 2018).

Staff members are responsible and accountable for all activities carried out under their username. No staff member shall jeopardise the integrity, performance or reliability of computers, networks, software and other stored information that are the property of the School. In this policy, "software" is taken to comprise programs, routines, procedures and their associated documentation which can be implemented on a computer system, including personal computers and laptops.

School staff who are authorised to access data are subject to strict ethical standards as a condition of their employment. No staff member shall interfere or attempt to interfere in any way with information belonging to another person. Similarly, no person shall make unauthorised copies of information belonging to another person. The School will routinely monitor its data traffic flows (and reserves the right to monitor individual use) to maintain operational continuity and to ensure that resources are appropriately used. Staff should be aware that Internet services used via the School network are logged and monitored. The School will routinely monitor staff emails to ensure appropriate use of the facility is maintained.

Any software and/or hard copy of data or information which is not provided or generated by the user personally and which may become available through the use of computing or communications resources shall not be copied or used without permission of the school, or the provider of the software.

The member of staff must not undertake any actions that bring the name of the School into disrepute. Staff members who are in breach of this policy may find themselves subject to School disciplinary and/or criminal procedures.

4. Legal Responsibilities

Staff members undertake not to infringe any copyright in documentations and/or software. The Copyright, Designs and Patents Act in 1998 gives copyright owners the right to bring civil proceedings for infringement and makes certain infringements of copyright criminal offences.

Staff members undertake not to use any School computing or network resources to make use of or publish material that is obscene, libellous or defamatory or in violation of any right of any third party or in violation of the Schools Codes of Practice concerning harassment.

Staff members undertake to comply with the provisions of the Computer Misuse Act (1990), Criminal Justice and Public Order Act 1994, the Data Protection Act (1998) and other relevant statutes.

5. Security

No electronic communications system is 100% secure; e-mail and internet use is particularly susceptible to interception, corruption and the "infection" of malware. That said, the School will take whatever measures are deemed appropriate and reasonable to ensure a safe environment for use by pupils and staff.

The computer facilities in the School are monitored to ensure compliance with this Policy via automated appliances that tracks unacceptable usage, and by periodic checks by the Head

of ICT. This appropriate level of filtering is applied to at website, image and key word filtering to restrict access to radicalisation, hate and radicalisation content in particular.

The integrity of the School's computer systems is jeopardised if users do not take adequate precautions against malicious software, also referred to as malware. Staff should be aware that email is used to carry malware and ransomware in attachments, may be used to "phish" confidential and secure data from the recipient. If you are in any doubt do not open the email and contact a member of the IT Department who will be able to assist you. External devices such as hard disk drives or key drives must be checked for viruses before being connected to a school computer using the anti-virus software provided by the School. The ability to undertake a particular action does not imply that it is acceptable. Existing norms of behaviour apply to computer based information technology just as they would apply to more traditional media. Examination of all files in the folder of a fellow staff member is equivalent to examining their filing cabinet and seeking to find unprotected files on a multi-user system falls into a similar category.

Every effort is made to ensure that there is no incidence of cyber-bullying using equipment supplied by the School. Reference should be made to the Anti-Bullying Policy for specific reference to Cyber-Bullying.

Network Accounts

As a member of the Elstree School staff, you are allocated a network account that enables you to access network resources. Permissions for various resources on the network are prescribed to each account and maybe accessed using the username and password that is allocated to that account. Each account is for the exclusive use of the person to whom the account has been allocated. Attempts to access or use any account which is not authorised for your use are prohibited. The password associated with a particular network account must not be divulged to another person. After authenticating themselves, staff should not leave their computer unattended without password protection or logging off the computer.

Staff must ensure the confidentiality of their account passwords. Passwords should be changed regularly and not written down. They must not be shared with others either inside or outside the School. Passwords should be chosen carefully, and should ideally be a combination of letters and numbers that are not immediately associated with the individual, for example, passwords that consist of phone numbers, dates of birth, names of spouse or pets, and similar 'guessable' words or phrases must not be used. Computer users should 'log-off' each time they finish using a computer to prevent unauthorised access.

Confidentiality

It is to be noted that all information relating to pupils and staff at the school must remain confidential at all times. Care should be taken to ensure any portable computing equipment containing such information is secure, particularly when off the school premises. If there is school data on your device it must be encrypted and only retained for the amount of time required. For example when writing reports at home on your laptop all details must be erased as soon as the reports are finalised. You will be in breach of the Data Protection Act if any such data becomes available to anyone outside of the school whilst in your possession and you should note there are significant penalties for such a breach.

6. Social Media

The internet provides a range of social media tools that allow users to interact with one another, for example, rediscovering friends on social networking sites such as Facebook, keeping up with other people's lives through Twitter and maintaining pages on internet encyclopaedias such as Wikipedia.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

This policy applies to personal web space such as social networking sites (e.g. Facebook, MySpace, Instagram, SnapChat), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

In using social networking and internet sites, clear and explicit professional boundaries will be adhered to as outline in Section 12 of the DCSF Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings, which can be found at the following link http://www.childrenengland.org.uk/upload/Guidance%20.pdf.

Principles

Staff members must be conscious at all times of the need to keep their personal and professional lives Separate. They should not put themselves in a position where there is a conflict between their work at Elstree School and their personal interests.

i. Staff members must not engage in activities involving social media which might prejudice adversely the interest or reputation of Elstree School.
ii. Staff members must not represent their personal views as those of Elstree School on any social medium.
iii. Staff members must not discuss, disclose or refer to personal information about pupils, staff and others they interact with as part of their employment on any social media.
iv. Staff members must not use social media and the internet in any way to attack, insult, abuse or defame staff and pupils, their family members, colleagues, and other organisations or undertakings doing business with Elstree School.
v. Staff members must act in good faith and be accurate, fair and transparent when creating or altering online sources of information on behalf of Elstree School.

Personal Use of Social Media

Staff members must at all times ensure that they cannot be identified as an as employee of Elstree School or service provider for the school or contractor in their personal use of the internet/cloud services. This is to prevent information on these sites and services from being linked with the school and to safeguard the privacy of staff members, pupils and parents.

Staff members must not have contact through any personal social medium with any pupil, whether from Elstree School or any other school, unless the pupils are family members. Staff may not be friends with any ex-pupil until they reach the age of 18.

Elstree School does not expect staff to discontinue contact with their family members via personal social media once the school starts providing services for them. However, information staff have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other individuals, organisations or

undertakings doing business with Elstree School must not be discussed, disclosed or referred to.

Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

If a staff member wishes to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created.

Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these with their line manager and signpost pupils to become 'friends' of the official school site.

On leaving Elstree School, staff members must not contact current Elstree School pupils by means of personal social media sites. Similarly, staff members must not contact current pupils from their former schools by means of personal social media.

Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other individuals, organisations or undertakings doing business with Elstree School must not be discussed, disclosed or referred to on their personal web space.

Photographs, videos or any other types of image of pupils and their families or images depicting staff wearing school uniforms or clothing with school logos or images identifying school premises must not be published on personal social media and internet sites.

School or email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Elstree School logos or brands must not be used or published on personal social media or internet sites.

Elstree School permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the School as their employer.

Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly then the settings on the site imply. Any reference to such information by pupils and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to their line manager in the first instance.

If a member of staff becomes aware that a pupil (or group of pupils) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they must report this to the Headmaster so that the appropriate process can be followed.

Using Social Media on Behalf of Elstree School

Staff members must only use official school sites for communicating with pupils or to enable pupils to communicate with one another.

There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff members must not create sites for trivial reasons which could expose Elstree School to publicity that is likely to adversely damage or harm the interests of the school or its reputation. The Headmaster must be consulted before any member of staff embarks upon such a venture. The Deputy Headmaster and the Registrar have full responsibility for running the official Facebook, Flickr, Twitter and Vimeo sites. No other social media platforms may be set up by any staff member which has a direct or indirect connection with Elstree School.

Official school sites must be created only according to the requirements specified. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

Staff members must at all-time act in the best interests of Elstree School, children and young people when creating, participating in or contributing content to social media sites.

Monitoring of Internet Use

Elstree School monitors usage of its internet and email services without prior notification or authorisation from users.

Users of Elstree School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's network system.

Breaches of Policy

Any breach of this policy may lead to disciplinary action being taken against the staff member involved in line with the Disciplinary Policy and Procedure.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Elstree School or any illegal acts or acts that render Elstree School liable to third parties may result in disciplinary action or dismissal.

7. Use of Mobile/Smart Phones and Personal Mobile Devices

Introduction

Children have their photographs taken on school cameras and downloaded onto the school system to provide evidence of their achievements for developmental records **(The Early Years Foundation Stage, EYFS).**

Staff, visitors, volunteers and students **(within the Early Years Foundation Stage, EYFS)** are not permitted to use their own mobile devices to take or record any images of Elstree children for their own records during session times.

Only school cameras and video equipment is used to record children in the Early Years. No photographs or videos are allowed to be taken on staff mobile phones. Photographs and recordings of children are only taken for valid reasons, i.e. to record their learning and development, or for displays within the setting.

This applies to our EYFS and after school care.

Procedures

Under the Data Protection Act 1998, Elstree School must seek parental consent to take still and moving images. Images will be stored on the School's servers which is password protected. If the School ceases to operate, all photographs will be shredded or deleted from the School system.

Elstree's digital cameras or memory cards must not leave the school premises except for use on school trips. Photos are uploaded to the School servers or printed in the setting by staff and images are then removed from the camera's memory.

Photographs may be taken during indoor and outdoor play and displayed in albums or a child's development records for children and parent/carers to look through.

Often photographs may contain other children in the background.

Events such as, Sports day, Outings, Christmas and Fundraising Events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending. Parents should not share images/video on social media without prior permission from parents of the children involved.

On occasion we might like to use photographs of the children taking part in an activity to advertise/promote our school via our Web site etc.; in accordance with parental permission.

Staff may use their phones/personal devices to take photos of school events on the strict understanding that these are downloaded onto the school system (within 24 hours) and deleted off their personal devices. Personal devices should only be used if the school camera is not available.

Staff mobile phones / personal devices must only be used to access emails in staff areas and not in the presence of children. Staff may occasionally use their phones/personal devices to take photos of school events on the strict understanding that these are downloaded onto the school system (within 24 hours) and deleted off their personal devices. Personal devices should only be used if the school camera is not available.

Cameras and mobile phones are prohibited in the toilets or changing areas.

In cases of a personal emergency all personal calls should be directed through the Elstree office phone.

Staff are asked not to make personal calls during their working hours. However, in urgent cases, a call may be made or accepted if deemed necessary and by arrangement with the Headteacher.

Any non-compliance will be taken seriously, logged and investigated appropriately in line with our disciplinary policy.

8. Communications

Accidental eMail

E-mail is also easily transmitted, perhaps unintentionally, by the accidental pressing of a key or click of a mouse. Partial or incorrect information transmitted in this manner could have adverse effects on the School business and care should be taken to ensure that this does not occur.

Legal Status

The law holds that e-mail, or a printout of an e-mail, has the same status as any other document and can be used as evidence in legal proceedings; as much care should be taken in the drafting of e-mail as with any other written communication.

The school's standard format for e-mail messages should be used where possible, and the 'classification box' should be completed where appropriate, e.g. 'CONFIDENTIAL'. The consent of the addressee should be obtained before confidential messages are sent via electronic systems.

Defamation and Harrassment

The more relaxed, open nature of e-mails makes it easy to communicate either directly, or by implication, something that could be construed as defamatory or as a form of harassment. Care must be taken in formulating messages to ensure that this does not occur, and staff should take great care in the drafting of any messages. Care should also be taken when forwarding messages from others.

Viruses

Viruses can be introduced into electronic communications systems through the use of corrupt computer discs or imported e-mail. These viruses can cause great disruption and incur considerable expense, in both time and money, for the School, and staff should take great that this should not occur. Staff should immediately delete suspicious e-mails from their inbox **without opening them** if uncertain of where the message has come from, and they **should not open attachments** unless they are absolutely certain that they are from a trusted source.

9. Personal Devices

Personal Computing Equipment

Advice should be taken from the Head of ICT before connecting any personal computing equipment to the school network. It may be necessary to install anti-virus software on computers or laptops belonging to staff if they are to be connected to this network.

Personal Computer Media

Staff must take care when bringing computer media from outside the school that such computer media is not contaminated by a virus. Virus scanning software provided by the school should be used for this purpose.

Mobile Devices

Mobile devices may be used in the classroom as part of a lesson but must be set to silent and must not be used for personal business (email, messaging, social media) in the presence of the children. Members of staff should respect the Staff Common Room and Work Room, and be mindful of other colleagues before using private mobile device.

Use of Phones

Every effort should be made to restrict the private use of mobile phones to the employee's own time. School phones should not to be used for personal calls.

10. Copyright

The copying of information electronically from any source, such as e-mail messages, web pages or computer media, may constitute copyright infringement. Staff must ensure that written permission has been obtained from the owner of the information before any such copying is done. Staff must also ensure that computer software is not copied unlawfully onto either school or personal computing equipment, and advice should be taken from the Head of ICT regarding the ability to legally copy software that has been purchased by the school.

11. Pornography and other Unsuitable/Inappropriate Material

The distribution of pornographic images or other unsuitable material gives rise to criminal liability under the Obscene Publications Act 1959 and other associated legislation. The access of illegal material electronically using computing facilities may lead to instant dismissal, and may also involve notification to the police.

Any staff member that receives inappropriate, unsuitable or illegal material via the e-mail system MUST notify the Headmaster and the Head of ICT IMMEDIATELY.