clarior ex obscuro

Elstree School

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

Acceptable Use Policy for IT

Person responsible for Policy: GW/TDW   Responsible Governor: Gavin Owston
Date of last revision: September 2023
Date to be revised: September 2025

Elstree School is a Company Limited by Guarantee No 690450 (England)

Registered Charity No 309101

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

The School will adopt a ***zero tolerance approach*** *to any cyber bullying, issues, that all staff will challenge any abusive behaviour between peers that comes to their notice and will report to the DSL immediately any issues of this nature. Please see the* ***Safeguarding and Prevent Policy*** *for further details about dealing with Peer-on-Peer abuse.*

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are each user's responsibility. Passwords need to adhere to the school password policy to be accepted and should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Department.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Head of Digital Learning.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies.

Staff are permitted to use personal devices to receive 2 Factor Authentication codes and notifications for use with school services. Additionally, the Splicecom app (phone system) may be used to make and receive calls related to school business, as long as this is done discreetly and away from children.

Staff are permitted to have personal devices in school so long as they use them in Staff only areas or classrooms or when children are not present. In an emergency, personal mobile phones may be used to contact the appropriate services. **They must not be used upstairs in the dormitories, changing rooms or toilets.**

Staff may not use their phones/personal devices to take photos of school events. Until suitable alternative school phones are acquired, the following Staff are permitted to take photos on their personal phones, which are then transferred to the Marketing Department system and deleted immediately from the phone: DB; BD; OSI; ACTI; SCA; TDW; LJO

All Years 6, 7 and 8 have personal computers in school. This is on strict understanding that their computers are used responsibly and sensibly in lesson and prep time only. All personal computers must be enrolled in the school system with inTune, SENSO and Securly software installed (see 'Monitoring and Access' below). The Pupil devices are stored downstairs for charging, when not required in lessons The Year 7s and 8s charge theirs in their Common Rooms, the Year 6s devices are stored securely in Form Rooms. They should not be used in free time.

Any property owned by pupils (full boarders only) such as mobile phones and other devices must be handed into the Heads of Boarding at the start of term, end of exeats and half terms for safekeeping. Full boarders will have access to their devices in public areas (common rooms and library) on Wednesday evenings under supervision by the resident boarding staff. **They must not be used upstairs to the dormitories, changing rooms or toilets.**

Monitoring and access

Staff, parents and pupils should be aware that their use of technology (including, but not limited to: email / messaging, internet sites, file storage, O365 usage and including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes. The school employs screen monitoring software (SENSO), email security filters (O365) and web traffic filters Securly for the purpose. Web history, school email accounts and storage locations may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances.

The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies

You will ensure that you comply with the school's IT Policy, Safeguarding and Prevent Policy, Anti-Bullying, Cyber Bullying Policy and Staff Data Protection Policy.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be routinely deleted after **7 years** or kept in archive and email accounts will be closed [and the contents deleted / archived] within **1 year** of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information [(or indeed any personal information that they wish to keep, in line with school policy on personal use)] is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact Head of Digital Learning.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they should report it to **Graham Wootten, Head of Digital Learning**

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or you are concerned that a member of the school community is being harassed or harmed online you should report it to DSL or DDSLs.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the **Head of Digital Learning**.

I understand and accept this acceptable use policy (staff / pupils):

Name: …………………………………………………………

Signature: …………………………………………………………

Date: …………………………………………………………

For younger pupils (below secondary school age)

Name of parent/guardian: …………………………………………………………

Signature: …………………………………………………………

Date: ………………………………………………………….