Digital Strategy

Updated: April 2021

Owner: Head of Computing

Table of Contents

1. Core principles and delineation of responsibility

1.1 This policy should be read in conjunction with the following policies

1.1.1 Child protection and Safeguarding Policy
1.1.2 Engagement and Mood Management Policy
1.1.3 Staff Handbook

1.2 Digital technology helps pupils learn creatively and effectively. It encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The digital policy encourages appropriate and safe use of technology while maintaining a balance with traditional methods of teaching.

1.3 The promotion digital awareness is the responsibility of all members of staff and the wider community. Responsibility for the signposting of specific matters relating to digital safety is shared by the school's team of Designated Senior Persons under the leadership of the Designated Safeguarding Lead as detailed below.

1.3.1 The DSO and DSL will monitor and evaluate this policy. In the event of an incident, the following people may be informed within school:
1.3.2 Principal
1.3.3 Vice- Principal
1.3.4 Assistant Principal
1.3.5 Head of Computing the IT Support Team
1.3.6 Heads of Year (if appropriate)

2. Email and internet use

2.1 All internet activity must be appropriate to the pupil's education and be protected by an up to date internet management system.

2.2 Access should only be made via the authorized password, which must not be made available to any other person.

2.3 Activity which threatens the integrity of the School's digital systems, or activity which attacks or corrupts other systems, is strictly forbidden.

2.4 E-mail can only be used for legitimate school-based purposes. Limited use of email and Internet facilities for personal purposes is permitted. The School acknowledges that personal use may occur from time to time.

2.5 Use for personal financial gain, gambling, political purpose or advertising is strictly forbidden.

2.6 Use of the school address to deliver goods purchased online must be authorised by the principal first.

2.7 Copyright of materials must be respected. If information is obtained from the Internet, any directly quoted material must be clearly specified and its source listed in the bibliography.

2.8 Use of the network to create, distribute, store or access inappropriate matter, such as pornographic, racist or offensive material, is strictly forbidden.

2.9 Pupils must exercise discernment and report inappropriate material.

2.10 Pupils must understand that the network is monitored constantly and infringements will be reported to the relevant Head or Principal. Pupils contravening these guidelines will be removed immediately from the network and will be subject to the School's discipline code.

2.11 Programme files must not be downloaded or installed from an external source and must not be run from a USB data stick or other external storage device.

3. Use of Equipment

3.1 Pupils should be inducted by teachers annually on the safe and appropriate use of equipment. This should be repeated as necessary during the academic year

3.2 All BYOD (Bring Your Own Device) must adhere to the Acceptable Use Policy

3.3 Staff are expected to monitor the use of equipment and children must not be left unsupervised while using a device

3.4 Digital devices are not permitted for pupils during break, lunch or pick up time. Staff are not to be on their personal device while supervising pupils. Use of a staff iPad is permitted

3.5 Any such use of a device must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of devices will be dealt with through the disciplinary procedure.

3.6 All devices must be locked with an active passcode before being left unattended
3.7 The creation or transmittance of any material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, is strictly prohibited
3.8 The transmittance of any material such that the copyright of another person is infringed is strictly prohibited.
3.9 The transmittance of any confidential information of the School otherwise than in the normal course of duty or instruction is strictly prohibited
3.10 No person is permitted to download any files unless virus scanned;
3.11 No person is permitted to gain deliberate unauthorised access to facilities, or devices
3.12 No person is permitted to send any message internally or externally which is abusive, humiliating, hostile or intimidating
3.13 No person is permitted to disclose passwords to third parties without the consent of the School
3.14 All persons must observe this policy at all times and note the disciplinary consequences of non-compliance which in the case of a gross breach or repeated breach of the Policy may lead to dismissal or expulsion
3.15 Equipment brought to the school is done so at the risk of the owner and the school will not be responsible for loss or damage

4. Communication Guidelines

4.1 Monitoring communications

4.1.1 The School reserves the right to monitor staff and pupil communications held on its platforms in order to:
4.1.2 Establish the existence of facts
4.1.3 Ascertain compliance with regulatory or self-regulatory procedures
4.1.4 Monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes.
4.1.5 Prevent or detect crime
4.1.6 Investigate or detect unauthorised use of the School's telecommunication system
4.1.7 Ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding emails to correct destinations.
4.1.8 Gain access to routine business communications, for instance checking voice mail and email when staff are on holiday or on sick leave
4.1.9 Parents or children using social media to defame the school or its community will be investigated
4.1.10

4.2 Cyber Bulling

4.2.1 Bullying is the act of intentionally causing harm to others, through verbal harassment, physical assault, or other more subtle methods, i.e. exclusion from a group or spreading rumours, etc.

4.2.2 Cyber bullying is bullying using technology. This means things like prank calling, sending nasty text messages and posting on hate sites, as well as forwarding hurtful emails, sending round humiliating videos, photos, and any other digital media

4.2.3 Pupils and staff must be provided a safe way of reporting inappropriate communications

4.2.4 Using the School's network, or a personal mobile phone, or a home PC, to send out messages, images, online posts, SMS messages, phone calls, or any other type of digital communication that undermines, intimidates, upsets, or disturbs, another student, or a member of staff, will be considered to be cyber bullying. The School makes no differentiation between bullying that occurs via digital means to bullying that occurs in person, and any incidence of cyber bullying will be dealt with severely. The following are or must be monitored carefully by the relevant person.

- Social Networking Sites
- Instant Messaging Services
- Gaming
- Phones
- Webcams
- Forums and Message Boards

4.3 Good Practice

4.3.1 Digital communication can be a vital tool of communication but must be used to positively improve communication experiences of all those who interact electronically

4.3.2 Communications should be limited to reasonable hours and circumstances. Avoid sending communication 'out of hours'

4.3.3 Is your communication necessary, better in person, or simply at a different time? People are busy. Your message may be one of tens or hundreds for a recipient to deal with. For many people, email becomes a chore, not a vital tool of communication. Please do not add to this by sending messages/information that could be communicated in another, often more efficient, way

4.3.4 Communication with staff is restricted to between 6am and 6pm unless SLT deem it necessary

4.3.5 If emails are of a disciplinary nature, then think twice. Sometimes this allows time to digest and is better than the ' please see me at the end of the day' and sometimes face to face is better

4.3.6 If your email exchange on one topic results in two or more "cycles", then it is probably best to stop and talk to each other

4.3.1 If you have something to 'get off your chest', write the email message and then save it. Let it lie for a few hours or a day and then re-read it. In the meantime, circumstances may change or you may have an opportunity to talk to the person(s) involved

4.3.2 Before responding to any e-mail message, re-read it to ensure that you fully understand it

4.3.3 Short paragraphs. Keep your paragraphs short so your emails can be read quickly by busy people

4.3.4 Use emoticons appropriately

4.3.5 Consider carefully before forwarding a message and to whom. Take great care with any attachments, even from senders well known to you.

4.3.6 Don't be that person. Reply All is for use when you want to send a response to the person who sent you the email AND everyone else they sent it to.

4.3.7 The use of WhatsApp is not as private as you might think. Don't send messages you may later regret.

5. Keeping yourself and others safe

5.1 Don't post content that is very personal – keep information general.

5.2 Think carefully about posting pictures online – once it's there, anyone can see it or use it.

5.3 Keep your personal information private.

5.4 It's not a good idea to meet up with someone you meet online – you don't really know who they are.

5.5 Try to think carefully before you write things online – people can get the wrong end of the stick.

5.6 Respect other people's views – just because you don't agree with them, it doesn't mean you have to be rude or abusive.

6. Social Media

6.1 Usage

6.1.1 Any platforms that use a form of social interaction must be risk-assessed by the school, or teacher in charge, prior to any lesson to ensure it is age-appropriate and safe for use.

6.1.2 Staff members are required to have private social media accounts.

6.1.3 Private Twitter or social media posting using media generated from the school may be monitored and if deemed necessary, required to be taken down by the relevant member of staff.

6.1.4 Staff must demonstrate an awareness of their role in the community and be mindful of any content posted on social media and the impact it may have, regardless of intention.

6.1.5 Staff and pupils must recognise the important role of the school in the life of the local community, and take responsibility for upholding its reputation and building trust and confidence in it.

6.1.6 No contact is permitted between ex or current pupils and staff members on social media. Any such attempted contact should be reported to Safeguarding team within 24 hours.

6.2 Appropriate age for use of social media

6.2.1 In accordance with the terms and conditions of many popular social networks (e.g. Facebook), the School recommends that no children, under the age of 13, should have publicly visible social media accounts.

6.3 Use of pupil imagery

6.3.1 When using school sanctioned accounts, staff should ensure they only publish images when parental permission has been granted.

6.3.2 Pupil surnames should not be included in any comments, messages or posts.

6.3.3 The School will minimise the risk to children of putting images of pupils on Social Media through the following steps:

- Staff should endeavour to avoid posting full face photos of happy smiling pupils (because full face photos can be cropped more easily onto other images).
- Staff should take photos of pupils from the side or from an angle, heads down or from a distance. In this way schools can still display images of happy and industrious pupils.
- Staff must not use full names of pupils or specify the year group.
- The principle of "Faces without Names; Names without Faces" should apply.
- Staff may take photographs of pupils for use on social media so long as they don't store them on their phones or devices – i.e. the image must be deleted within 24 hours.

7. Mobile Phones

7.1 Unless being used for a teaching and learning activity, phones should not be used while supervising pupils

7.2 Pupils must have written consent to bring a mobile to school and it must remain with the teacher

8. Complience

8.1 Instances of proven and intentional breach of the above will result in sanctions that may include suspension from the school or refusal to re-enrol the pupil for the next academic year (as per the KHDA contract); staff members also have the right to inform the police where they have been subjected to public defamation of character.