# SEAHAM HIGH SCHOOL

# Acceptable Use Policy
# Including social media guidance

| Review date | Cycle | Reviewer | Adopted | Committee |
|---|---|---|---|---|
| September 2022 | Annually | Data Protection Officer | November 2022 | Full Governors |
| September 2023 | Annually | Data Protection Officer | December 2023 | Full Governors |

## Contents

1. Introduction and aims ..... 3
2. Relevant legislation and guidance ..... 3
3. Definitions ..... 4
4. Unacceptable use ..... 4
5. Staff (including trustees, volunteers, and contractors) ..... 6
6. Students ..... 11
7. Parent/carers ..... 12
8. Data security ..... 12
9. Internet access ..... 15
10. Cyber attacks……..……..10
11. Monitoring and review ..... 16
12. Related policies ..... 16
Appendix 1: Facebook cheat sheet for staff ..... 17
Appendix 2: Acceptable use of the internet: agreement for parent/carers and carers .. 20
Appendix 3: Acceptable use agreement for older students.....**Error! Bookmark not defined.**
Appendix 4: Acceptable use agreement for younger students ..... 21
Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors ..... 22

## 1. Introduction and aims

The purpose of the policy is to ensure the school network is operated safely and all users of IT are safe. It refers to our school IT network and to the use of mobile technologies, both within it and external to it, explains the behaviours which are acceptable and unacceptable within our school.

IT is an integral part of the way our school works, and is a critical resource for students, staff, trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the IT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school IT resources for staff, students, parent/carers and trustees
- Establish clear expectations for the way all members of the school community engage with each other and with stakeholders online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of IT systems
- Support the school in teaching students safe and effective internet and IT use

This policy covers all users of our school's IT facilities, including trustees, staff, students, volunteers, contractors and visitors.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face disciplinary action and in the most serious cases legal action may also be taken.

## 2. Legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- The UK General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990

- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011

## 3. Definitions

- **"IT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, communication applications such as WhatsApp, Facebook messenger, SMS messaging and any device system or service which may become available in the future which is provided as part of the IT service
- **"Users":** anyone authorised by the school to use the IT facilities, including trustees, staff, students, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities
- **"Materials":** files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

## 4. Unacceptable use

The following is considered unacceptable use of the school's IT facilities and online platforms by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Activity which defames or disparages the school or trust or risks bringing the school/trust into disrepute
- Sharing confidential information about the school, its students, or other members of the school/trust community
- Connecting any device to the school's IT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data
- Gaining, or attempting to gain, access to restrITed areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities
- Causing intentional damage to IT facilities
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school/trust
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or other delegated member of SLT will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the IT facilities.

### 4.1 Exceptions from unacceptable use

Where the use of IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

In such circumstances, permission must be sought from the headteacher or delegated member of SLT.

### 4.2 Sanctions

Staff or students who engage in any of the unacceptable activity listed above may face disciplinary action in line with our policies including the Behaviour Policy (Students), Disciplinary Policy and Staff Code of Conduct (Staff).

In the case of adults who are not staff members other sanctions are available such as revoking permission to use the school's systems.

Members of staff will have been provided access to the above policies as part of your induction. If you require access to a copy these are available from the school office.

## 5. Staff (including trustees, volunteers, supply teachers and contractors)

### 5.1 Access to school IT facilities and materials

The school's headteacher oversees access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact a member of SLT or the IT department.

#### 5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parent/carers and students, and must not send any work-related materials using their personal email account.

E-mail attachments should only be opened if the source is known and trusted. There have been an increasing number of spam emails received by staff in schools which contain links that can be damaging to IT systems and also lead to serious network and equipment hacking.

If you are required to send an email to more than one recipient, ensure that the email addresses are entered in to the 'bcc' box to ensure that you are not sharing personal email addresses with others.

E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable and public.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. A double checking system should also be implemented whereby one member of staff asks another to check content of their message before sending

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the school business manager or data protection officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parent/carers or students. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4.

If for any reason a member of staff feels there is a need to attempt to record a telephone conversation this should be discussed first with the headteacher or an appropriate member of SLT.

**5.1.2 Use of printers**

Staff should take care when printing on central printers located in the school. Confidential documents or those containing personal information relating to others should not be printed at a time when they cannot be immediately removed from the printing facilities. Where printer logins are provided these should be used at all times.

### 5.2 Personal use

Staff are permitted to occasionally use school IT facilities for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused. The school may withdraw permission for it at any time or restrIT access permissions.

IT facilities personal use is permitted provided that such use:

- Does not take place during worktime
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the school's IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of IT (even when not using school IT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parent/carers could see them.

Personal mobile phones should not be used in areas of school where students have access.

Mobile phones should be switched to silent mode and kept out of sight during the school day. Staff are allowed to access their personal phones on breaks, lunch times and after school when students are not present. It is also permissible to use mobile phones to access passcodes for dual authentication systems.

It is forbidden to take photographs/videos of students on personal mobile phones. School supplied equipment should always be used for these purposes.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

#### 5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Remember that damage to professional reputations can inadvertently be caused by quite innocent postings or images.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

### 5.2.2 Communication platforms

Members of staff should consider how they communicate with each other both inside and outside of school when discussing any work matters. This includes during personal time on messaging platforms such as Whatsapp and Messenger. Remember that what you may deem as 'personal' messages could unintentionally become public and therefore if school matters are being discussed you should consider carefully your use of language and subject matter.

School will always encourage staff that any messages relating to school, even in 'personal' forums should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

## 5.3 Remote access

We allow staff to access the school's IT facilities and materials remotely through Google drive and our cloud based platforms.

Staff accessing the school's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and take such precautions as the school may require from time to time against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

No school related information should be stored on any personal equipment. You must not download or save any information onto personal equipment such as mobile phones or laptops/PCs.

If you have a need to work offsite and require electronic or paper based information to be taken from school to work on you must

- First seek permission from the head teacher or delegated member of SLT for the removal of the information eg student file, laptop, encrypted school memory stick
- Ensure the secure transit of the information

- Ensure that no information is downloaded or stored on personal equipment
- Be aware of other people within the immediate area when viewing personal or sensitive information in areas outside of school and limiting such activity away from public places

### 5.4 School social media accounts

The school has guidelines for what can and cannot be posted on its social media accounts and staff must ensure they abide by these guidelines at all times. Staff must ensure students have consent before posting photographs of them onto social media.

### 5.5 Images of students

Students need parent/carers permission to have photographs or videos published electronically or in a public area even if they are unidentifiable. If in doubt as to whether a student has permission you must check with the school office before publishing/displaying.

No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Images of students must be stored in the designated area of the IT network/Cloud. It is not permitted to remove images off site (on camera, phone or storage device).

Images should be deleted from electronic devices once after uploading to the above storage area.

### 5.6 Monitoring of school network and use of IT facilities

The school reserves the right to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors IT use in order to:

- Obtain information related to school business

- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

## 6. Students

### 6.1 Access to IT facilities

- Activities should be planned by staff so that 'open searching is kept to a minimum.
- Computers and equipment in school are available to students only under the supervision of staff
- When searching the internet with students, adults should encourage students to use 'child safe' search engines if applicable (depending on age)

### 6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for any data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

### 6.3 Unacceptable use of IT and the internet outside of school

The school will sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on school premises):

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restrITed areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities
- Causing intentional damage to IT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

## 7. Parent/carers/carers

### 7.1 Access to IT facilities and materials

Parent/carers do not have access to the school's IT facilities as a matter of course.

However, parent/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at our discretion.

Where parent/carers are granted access in this way, they must abide by this policy as it applies to staff.

### 7.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parent/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parent/carers to sign the agreement in appendix 2.

## 8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parent/carers and others who use the school's IT facilities should use safe computing practices at all times.

### 8.1 Passwords

Each adult working within the school must log on to the computers using the username and password given to them (class account or individual account) and these must be changed to an individual specific password where stated. Passwords need to be kept a secret, not written down and stored in or around the computer. If for any reason an adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.

Any supply teachers or visitors to the school must obtain a guest account and password. Their password will need to be kept private and not shared.

You should ensure you use dual factor authentication when possible if dealing with sensitive information.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parent/carers or volunteers who disclose account or password information may have their access rights revoked.

### 8.2 Software updates, firewalls, and anti-virus software

All of the school's IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's IT facilities.

Any personal devices using the school's network must all be configured in this way.

### 8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. Data protection policy requires that any staff or student / student data to which members of staff have access, will be kept private and confidential, except when it is deemed necessary that by a requirement of law or by school policy to disclose such information to an appropriate authority.

### 8.4 Access to facilities and materials

All users of the school's IT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert a member of SLT immediately.

Users should always log out of systems and lock their equipment when they are not in use or when they leave the room, to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

### 8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption. Therefore, personal equipment such as USB sticks or other personal devices are not permitted. School adopt dual authentication for access to some identified systems and programmes such as email accounts and CPOMS.

## 9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with trustees and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software

    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data on a regular basis and store these backups on cloud based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure IT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

## 9. Internet access

The school wireless internet connection is secured and content filtering is in operation. If you should happen to access an inappropriate site that the filter has not identified, or 'safe' sites that are filtered in error, please inform a member of SLT or IT Technician.

### 9.1 Parent/carers and visitors

Parent/carers and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted.

Authorisation will only be granted if;

- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Parent/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

## 10. Monitoring and review

The School Business Manager and Data Protection Officer monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The Governors are responsible for approving this policy.

## 11. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour Policy
- Disciplinary Policy
- Data protection Policy
- Use of Photographic Images Policy
- Staff Code of Conduct

## Appendix 1: Facebook guidance sheet for staff

**Don’t accept friend requests from pupils on social media**

### 12 rules for school staff on Facebook

1. Consider changing your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile pITure to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your students
6. Don’t use personal social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your students online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parent/carers or students)
11. Consider very carefully any friend requests from parent/carers/carers
12. Never use facebook to respond to parent/carers/carers regarding queries or questions around school business

---

### Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, students and their families may still be able to read your posts, see things you’ve shared and look at your pITures if they’re friends with anybody on your contacts list

- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile pITure, cover photo, user ID (in the URL for your profile), country, age range and gender

## What do to if…

### A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile pITure
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parent/carers. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

### A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:

    - Responding to one parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Students may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
    - Parent/carer's sometimes feel that they can contact you through your personal facebook account to ask questions or raise issues in relation to school. To respond to such communication would be in breach of school policies

- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

### You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

## Appendix 2: Acceptable use of the internet: agreement for parent/carers and carers

| Acceptable use of the internet: agreement for parent/carers and carers | |
|---|---|
| **Name of parent/carer/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parent/carers/carers to communicate with, or about, our school.<br><br>The school uses the following channels:<br><br>• Our official Facebook page<br>• Email/text groups for parent/carers (for school announcements and information)<br>• Our virtual learning platform<br><br>Parent/carers/carers also sometimes set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp). Please note that school has no responsibility for the running or content for such groups. | |
| When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:<br><br>• Be respectful towards members of staff, and the school, at all times<br>• Be respectful of other parent/carers/carers and children<br>• Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure<br><br>I will not:<br><br>• Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way<br>• Use private groups, the school's Facebook page or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident<br>• Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parent/carers/carers | |
| **Signed:** | **Date:** |

## Appendix 3: Acceptable use agreement for students

| **Acceptable use of the school's IT facilities and internet: agreement for students and parent/carers/carers** | |
|---|---|
| **Name of student:** | |
| **When I use the school's IT facilities (like computers and equipment) and get on the internet in school, I will not:**<br><br>• Use them without asking a teacher first, or without a teacher in the room with me<br>• Use them to break school rules<br>• Go on any inappropriate websites<br>• Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)<br>• Use chat rooms<br>• Open any attachments in emails, or click any links in emails, without checking with a teacher first<br>• Use mean or rude language when talking to other people online or in emails<br>• Share my password with others or log in using someone else's name or password<br>• Bully other people<br><br>I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.<br><br>I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.<br><br>I will always be responsible when I use the school's IT systems and internet.<br><br>I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them. | |
| **Signed (student):** | **Date:** |
| **Parent/carer/carer agreement:** I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer/carer):** | **Date:** |

## Appendix 4: Acceptable use agreement for staff, trustees, volunteers and visitors

| **Acceptable use of the school's IT facilities and the internet: agreement for staff, trustees, volunteers and visitors** | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| When using the school's IT facilities and accessing the internet in school, or outside school on a work device, I will not:<br><br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>• Use them in any way which could harm the school's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share my password with others or log in to the school's network using someone else's details<br>• Share confidential information about the school, its students or staff, or other members of the community<br>• Begin to use any new methods of collecting or storing personal or sensitive information- eg new apps which require input of students personal data without first seeking permission<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the school<br>• Delay in reporting any data breach as set out in the schools Data Protection Policy and breach procedure | |
| I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.<br><br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.<br><br>I will let the designated safeguarding lead (DSL) and IT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br><br>I will always use the school's IT systems and internet responsibly, and ensure that students in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

| TERM | DEFINITION |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/or enhance functionality. |
| **Pentest** | Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website. |

| TERM | DEFINITION |
| --- | --- |
| **Ransomware** | Malicious software that stops you from using your data or systems until you make a payment. |
| **Social engineering** | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| **Spear-phishing** | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |
| **Trojan** | A type of malware/virus designed to look like legitimate software that can be used to hack a vITim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programs designed to self-replicate and infect legitimate software programs or systems. |
| **Virtual Private Network (VPN)** | An encrypted network which allows remote users to connect securely. |
| **Whaling** | Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives. |