THE LION WORKS SCHOOL POLICY

# ICT acceptable use policy

| | |
|---|---|
| **Author of policy and position of responsibility:**<br>Justine Collinson, Headteacher | **Date policy finalised**<br>September 2024 |
| **Approved by:**<br>Bruno Davis, CEO | **Date of approval**<br>September 2024 |
| **Due to be reviewed:**<br>July 2025 | **Date of review:** |

Contents

## 1. Aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team) and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and board members
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including Board members, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Disciplinary policy, Positive Behaviour Support Policy and any other relevant policy.

## 2. Relevant legislation and guidance

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

- Independent School Standards Regulations 2014
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

## 3. Definitions

- **ICT facilities:** 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, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including Board Members, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by authorised personnel
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

## 4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT 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 programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted 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 ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

### 4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) 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.

### 4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour, discipline, staff discipline, staff code of conduct and safeguarding policies.

The school's policies are published and/or available on site or via the school's digital storage facilities that are available to all staff.

Misuse of ICT may result in the removal of access to ICT resources.

## 5. Staff (including Board Members and contractors)

### 5.1 Access to school ICT facilities and materials

The school's ICT Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Manager.

### 5.2 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 parents/carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as 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.

Staff must take extra care when sending sensitive or confidential information by email. Any external emails with attachments containing sensitive or confidential information must be encrypted so that the information is only accessible by the intended recipient.

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 that contains the personal information of another person, they must inform the ICT Manager and Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. 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 ICT acceptable use as set out in section 4. The school can record incoming and outgoing phone conversations.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

If a conversation is likely to require specific recording for record keeping purposes this can done on a school device with audio recording features. This should be discussed in advance with the Headteacher. If this is going to happen then all of those involved in the call must be aware that it is being recorded. The reasons for doing so could include:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

### 5.3 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The ICT Manager, with approval, may withdraw or restrict this permission.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT 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 ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Staff code of conduct.

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

Staff should take care to follow the school's guidelines on use of social media (see school's social media Policy) and use of email (see section 5) to protect themselves online and avoid compromising their professional integrity.

### 5.4 Personal Social Media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Please refer to the school's Social Media policy as well as appendix 1 of this policy for guidelines on social media security settings.

### 5.5 Remote Access

The school allows staff to access the school's ICT facilities and materials remotely. Staff using the school's resources remotely must abide by the same rules as those accessing the facilities materials onsite. Staff should exercise caution with this and should be mindful that unauthorised downloading of material on to personal devices is not permitted. It should also be noted that all material on the school's ICT systems that has been generated, edited or otherwise created by a member of school staff is the intellectual property of the school. Unauthorised sharing of this could result in disciplinary or legal action against any individuals concerned.

Our ICT 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. If in any doubt the user must contact the school's Data Protection Officer.

### 5.4 School Social media accounts

The school has an official Facebook, Instagram and Twitter account, managed by Ben Mitchell. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times. These can be found in appendix 7.

### 5.6 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

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

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards

- Ensure effective school and ICT 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

Our School Board has ultimate responsibly for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. The Headteacher will oversee this compliance and monitor the performance of the Designated Safeguarding Lead.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL, Headteacher and ICT manager, as appropriate.

## 6. Pupils

Pupils are provided with the following access to the school's ICT facilities:

- Laptop computers (either individually designated for use or shared machines)
- Tablets
- Desktop computers
- SMART boards

This access is permitted under supervision. Pupils are not provided with access to the school's wifi network other than when using the devices listed above.

### 6.1 Search and deletion

Members of the Senior Leadership Team are authorised to lawfully search and delete from student's electronic devices.

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the school, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Headteacher
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation, however if co-operation is not given then the search can proceed and Positive Behaviour policy will be followed

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher, or those authorised by the Headteacher, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

### 6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Positive Behaviour Support Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT 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 making 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
- Consensual or 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 pupils, or other members of the school community
- Gaining or attempting to gain access to restricted 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 ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

The full range of sanctions available to the school will be considered and a proportional response, as determined by the school, will be made.

## 7. Parents and Carers

Parents and carers do not routinely have access the school's ICT facilities and resources.

If parents or carers are granted access, for a specific purpose, they must abide by those guidelines and rules that are specified for staff use of the school ICT facilities.

### 7.1 Communicating with or about the school online

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

Parents and carers play a vital role in helping model this behaviour for their children, especially when communicating with the school or about the school online.

The school is always keen to have an open and candid dialogue with parents about any issues that arise. It should be noted that the school fully reserves the right to take legal action for any defamatory information that is communicated online about the school.

Significant or repeated defamatory, untrue or misrepresentative comments (as determined by the school) made online could be used as grounds to terminate a placement agreement. Reserving and/or exercising this right is fully compliant with the Independent School Standards regulations 2014.

### 7.2 Communicating with parents and carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

## 8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication

- Anti-malware software

### 8.1 Password

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. The requirements for a secure password are embedded in the password changing process and can not be circumvented by users.

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 pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Staff are prompted and required to change their passwords every 30 days.

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

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and 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 ICT 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.

### 8.4 Access to facilities and materials

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

These access rights are managed by the ICT manager.

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 ICT Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. This applies any time when a user walks away from a piece of ICT

equipment they are using. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

### 8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

## 9. Protection from cyber attacks

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

- Work with Board Members 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:
    1. Check the sender address in an email
    2. Respond to a request for bank details, personal information or login details
    3. 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:
    1. **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe or SWGFL) at least annually, to objectively test that what it has in place is effective
    2. **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    3. **Up to date:** with a system in place to monitor when the school needs to update its software
    4. **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be. These reviews will be done by, or overseen by the Headteacher. This may be delegated to the DSL, but effective compliance remains the responsibility of the Headteacher.

- Back up critical data at least weekly if stored offline and store these backups on non-networked external encrypted storage
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ICT Manager
- Make sure staff:
    1. Enable multi-factor authentication where they can, on things like school email accounts
    2. Store passwords securely using a password manager
- Make sure ICT 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
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

## 10. Internet Access

The school's wireless connection is secure.

There is internet filtering in place and response key stroke logging responses monitoring software. This software will notify Senior Leadership and DSL of any potentially harmful or inappropriate internet access.

Students are not permitted wifi access on personal devices.

### 10.1 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer)
- 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)

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

## 11. Monitoring and review

The Headteacher and ICT Manager will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

At each review this policy will be approved by the CEO with guidance and support from the School Board.

## 12. Related policies

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

- Online Safety
- Social Media
- Safeguarding and Child Protection
- Positive Behaviour Management
- Data protection

## Appendix 1: Facebook and social media Cheat Sheet for Staff

**DO NOT ACCEPT FRIENDS REQUESTS FROM PUPILS OR PARENTS ON SOCIAL MEDIA**

**10 Rule for school staff on Facebook or other social media platforms**

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure 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 happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils 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 parents or pupils)

### Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures 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 picture, cover photo, user ID (in the URL for your profile), country, age range and gender

### What to do if…

**A pupil adds you on social media**

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil 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 not appropriate to accept a friend request from a parent or carer from the school. Consult the school's Social Media policy of Staff code of conduct for more information.

**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 pupil or staff member notify the Headteacher immediately and the school can provide support, including through the school's behaviour and exclusions policy
- 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 parents

**Name of parent/carer:**

**Child:**

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Our official Instagram page
- The Arbor application
- Emails

The school is aware that parents/carers also 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).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- 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

I will not:

- 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 unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers
- I am aware that the school receives the right to take legal action in the event of defamatory, derogatory, misrepresentative or dishonest communication from a parent on social media or offline
- I acknowledge that action form the school could include termination of a placement agreement

**Signed:**

**Date:**

## Appendix 3: Acceptable use agreement pupils

| **Name of pupil:** | |
|---|---|
| When using the school's ICT facilities and accessing the internet in school, I will not:<br><br>- Use them for a non-learning and school reasons<br>- Use them without a teacher being present, or without a teacher's permission<br>- Use them to break school rules<br>- Access any inappropriate websites<br>- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)<br>- Use chat rooms<br>- Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>- Use any inappropriate language when communicating online, including in emails<br>- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video<br>- Share my password with others or log in to the school's network using someone else's details<br>- Bully other people<br><br>I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br><br>I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.<br><br>I will always use the school's ICT systems and internet responsibly.<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 (pupil)** | **Date** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer)** | **Date** |

## Appendix 4: Acceptable use agreement for staff and visitors (where applicable)

| **Name of staff member or visitor:** | |
|---|---|
| When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:<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 pupils or staff, or other members of the community<br>- Access, modify or share data I'm not authorised to access, modify or shar<br>- Promote any private business, unless that business is directly related to the school<br>- In anyway bring the school into disrepute | |
| I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<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>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil 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>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| **Signed** | **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. |
| **Breach** | When your data, systems or networks are accessed or changed in a non-authorised way. |
| **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. |
| **Pharming** | An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (such as 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 victim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programmes 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 people in an organisation. |

## Appendix 7: School Social Media guidelines for staff

### Social Media Use

Staff are reminded of their safeguarding statutory duties outline in KCSiE 2023. Staff need to ensure that their use of social media must also be acceptable and not blur personal and professional boundaries or leave your professional conduct in question.

Staff are not permitted to contact parents outside of school hours, nor on personal devices as this can leave them vulnerable and also blurs professional boundaries. It is accepted however that some staff may have existing relationships with parents of students who subsequently attend the school. In this instance professional judgement must be exercised. The school must not be brought into disrepute at any time and the confidentiality of all staff and student information must always be maintained.

On any social media platform, but especially Facebook, it is wise to check your privacy settings regularly and refer to the following advice:

- Change your display name so you are not easily identifiable.
- Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
- Be careful about tagging other staff members in images or posts
- Do not share anything publicly that you wouldn't be happy if your line manager, parents or students can see.
- Do not use social media sites during school hours
- Do not make comments about your job, your colleagues, our school or our students online.
- Do not associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
- Do not link your work email address to your social media accounts.

You can check your privacy settings on Facebook using the following advice and guidance:

- 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 have shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos – go to: https://www.facebook.com/help/236898969688346/?helpref=uf_share to find out how to limit the visibility of previous posts
- Google your name to see what information about you is visible to the public
- Remember that some information is always public; your display name, profile

picture, cover photo, user ID (in the URL for your profile), country, age range and gender

Under no circumstances should you accept a 'friend request' from a student. If you are contacted online by a student, please refer this matter at your earliest opportunity to a member of the Safeguarding team.

It would not be permissible to accept a 'friend request' from a parent of a student. This may leave you vulnerable and certainly blurs professional and personal boundaries. It is accepted that existing relationships with parents of students who subsequently attend the school may mean existing online connections. However, the staff member is responsible at all times for their conduct and should be mindful of professional expectations as well as those relating to the teacher or HLTA standards.

If you need any help with online safety or have any concerns about harassment or abuse, you can speak to our Online Safety Champion or any member of the Safeguarding Team. You may also find the following information useful:

- 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 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

**Gaming**

It should be noted that all rules relating to social media use and contact with students also applies to online gaming. It would never be acceptable to game against a student of the school online, or to communicate with them through such platforms. This blurs professional boundaries and is always inappropriate. In the event a member of staff unexpectedly finds themselves in contact with a student online in this way, it must immediately end and the Headteacher should be informed of it at the next appropriate opportunity. All efforts should then be made by the member of staff to block the young person from making further contact via the aforementioned means.