Blackfen School for Girls

Acceptable Use for School's ICT Network, School email and Internet Policy

Headteacher: Ms C Senior
Chair of Governors: Mr W Stone

	Date	Name	Signature	
Policy Date	February 2026			
Review Date	February 2027			
Review Period	Annually			
Lead Person	AHT Curriculum & Assessment	Nicola Hoad		
Prepared by	AHT Curriculum & Assessment	Nicola Hoad		
Verified by	Headteacher	Carrie Senior		
Approved by	Chair of Governors	William Stone		

Blackfen School for Girls

Rationale

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), governors, volunteers 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 governors
- 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 governors, staff, pupils, volunteers, contractors and visitors.
Breaches of this policy may be dealt with as outlined in the following policies: behaviour policy/staff discipline policy and or the staff code of conduct.

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

- 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
- Data (Use and Access) Act 2025
- 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 2025
- 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
- Meeting digital and technology standards in schools and colleges
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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 governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **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 5 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.

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 Artificial Intelligence (AI) Technologies and Generative Tools:

Artificial Intelligence (AI) technologies refer to any computer systems or applications that can perform tasks that typically require human intelligence. These include, but are not limited to:

- Generative AI tools that create text, images, audio, or video
- Conversational AI assistants and chatbots
- Predictive algorithms and automated decision-making systems
- Content creation and editing tools powered by machine learning

The following guidelines apply to all current and future forms of AI technology:

- Students must not use any AI technologies during assessments, including internal and external assessments, and coursework, unless explicitly permitted by staff for specific educational purposes.
- Students must not use any AI technologies to generate work that is submitted as their own without proper attribution and in accordance with the school's academic integrity guidelines. This includes text, code, images, audio, video, or other media created partially or wholly by AI tools.
- Students and staff must not input personal or confidential information into any AI technologies that could identify individuals associated with Blackfen School for Girls. This includes but is not limited to names, addresses, contact information, or any other personally identifiable data protected under UK GDPR.
- All users must exercise critical thinking when using AI-generated information and verify content through reliable sources.
- When AI tools are used for legitimate educational purposes, students should disclose their use and explain how the technology assisted their learning or work process.

The school recognises that AI technologies will continue to evolve rapidly. This policy covers all current and future AI tools, regardless of their specific names, brands, or developers. The school reserves the right to provide additional guidance on specific tools as they emerge and gain prominence in educational contexts.

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.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's network manager manages access to the school's ICT 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 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 team.

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. Staff must enable multi-factor authentication on their email account(s).

- 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 attachments containing sensitive or confidential information should be encrypted, where possible, 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 Data Protection Officer (DPO) immediately and follow our data breach procedure.
- Staff should not send such emails after 6:30pm on a school day at weekends or during School holidays and not before 7am in the morning.
- It is the prerogative of the Head Teacher to send emails outside of these hours when they deem it necessary for the smooth running of the school.
- There is an expectation that all staff check their emails at least twice a day, ideally before the start of School and at the end of the day. Staff are not expected to check emails after 6:30pm, before 7am. Staff are not expected to check emails when off sick or on leave.
- Emails should be responded to within 72 hours, even if the response is brief and promises a further later reply.
- Daily emails should be clear and concise.
- **Only reply to the original sender**; do not 'Reply all', unless absolutely necessary.

5.2 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 Headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours.
- 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 mobile phone policy.
- 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 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 make sure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely via the remote desktop services.

- The system is managed by IT Services Department.
- Access is restricted to Staff security group.
- Multi Factor Authentication is enabled and bound to account holder's mobile phone using Microsoft Authenticator app.
- Remote access rules are set out in this policy with emphasis on GDPR compliance. Additional security filters are applied to the system to prevent obsolete, outdate and unpatched devices using the system.
- Staff are offered remote access set up when they join. The main decision is whether they are willing to install the Microsoft Authenticator app on their phone.

Staff accessing the school's ICT 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 ICT facilities outside the school and must take such precautions as the network manager may require against importing viruses or compromising system security.

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.

5.4 School social media accounts

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 the relevant guidelines at all times.

5.5 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
- 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 governing board is responsible 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.
Where appropriate, staff may raise concerns about monitored activity with the school's DSL and IT network manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are generally accessed under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL:

  https://blackfenschoolforgirls.sharepoint.com/sites/StudentsDashboard/SitePages/CollabHome.aspx

- Sixth-form pupils can use the computers in the learning zone and study zone independently, for educational purposes only

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, 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 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)

Please see Screening, Searching, Confiscation Policy (Sept 2025) for further detail

6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour 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 such as copyright protected content
- Engaging in or interacting with cyber-crime of any sort, for example software piracy or hacking
- Utilising the school provided equipment to plan or exercise violence or taking part in criminal activities involving weapons, terrorism or any other anti-social behaviour
- 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

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.
However, parents/carers working for, or with, the school in an official capacity and may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.
Where parents/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 pupils, and help them learn, how to communicate respectfully with, and about, others online.
Parents/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 parents/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

We will inform parents/carers of online activity that their children are being asked to carry out as set out by **curriculum requirements provided by DofE**.

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 cyber-crime 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 work towards 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 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.
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.

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. Data Protection (GDPR) Policy (October 2024) Approved.pdf

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 network manager and the IT provider.
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 and the DPO immediately.
Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 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 network manager.

We don't enforce device encryption. We encourage using OneDrive or SharePoint so no data needs to travel on personal devices. OneDrive and SharePoint are encrypted.
GDPR also requires staff not print and take-home data unless absolutely needed to do so.

9. Protection from cyber attacks
Please see the glossary (appendix 5) to help you understand cyber security terminology.

- The school will:
- Work with governors 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 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 provided by the MSP at least annually, to objectively test that what it has in place is effective
- **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 effective and secure as they can be
- Back up critical data every night and store these backups on premises as well as in cloud-based backup system
- Delegate specific responsibility for maintaining the security of our management information system (MIS). Currently this is provided by Cantium.

Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts
- 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 – this is provided by LGFL
- 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 provider This plan will be reviewed and tested annually.

10. Internet access

- The school's wireless internet connection is secure.
- Add further details about your school's Wi-Fi arrangements. For instance:
- Whether you use filtering
- Whether you have separate connections for staff/pupils/parents or carers/the public
- If you use filtering, be aware that filters aren't fool proof. You may wish to include details of how to report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the relevant member of staff/service provider.

10.1 Pupils

- This is set out in this policy. Teachers who have computer suites or laptops in their departments, as well as Sixth Form staff inform students about the filtering and recording of their online activity.
- Students are restricted from inappropriate content on school's Wi-Fi which they see when they try search for such content

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's Wi-Fi 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
- Visitors need to access the school's Wi-Fi 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)

Add any other circumstances where parents/carers or visitors will be granted access to the internet.
Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review
The headteacher and DSL(s), AHT and network manager 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 annually.
The governing board is responsible for approving this policy.

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

- Online safety
- Safeguarding and child protection
- Behaviour policy
- Staff discipline
- Data protection
- Remote education
- Mobile policy
- Screening searches and confiscation
- Disaster recovery plan
- Teacher standards

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi 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 at your discretion whether to respond. Bear in mind that:
  - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- 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 pupil 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 parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Emails can be sent via Edulink and Sims InTouch. Text messages can also be sent Via Sims InTouch 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	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- 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
- Share my password with others or log in to the school's network using someone else's details
- Bully other people

When using Artificial Intelligence (AI) technologies and generative tools, pupils must not:

- use any AI technologies during assessments, including internal and external assessments, and coursework, unless explicitly permitted by staff for specific educational purposes.
- use any AI technologies to generate work that is submitted as their own. This includes text, code, images, audio, video, or other media created partially or wholly by AI tools.
- input personal or confidential information into any AI technologies that could identify individuals associated with Blackfen School for Girls. This includes but is not limited to names, addresses, contact information, or any other personally identifiable data protected under UK GDPR

All users must exercise critical thinking when using AI-generated information and verify content through reliable sources. When AI tools are used for legitimate educational purposes, pupils should disclose their use and explain how the technology assisted their learning or work process.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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.

I will always use the school's ICT systems and internet responsibly.

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, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • 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) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school • input personal or confidential information into any AI technologies that could identify individuals associated with Blackfen School for Girls. This includes, but is not limited to names, addresses, contact information, or any other personally identifiable data protected under UK GDPR	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. 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. 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. I will always use the school's ICT systems and internet responsibly, and ensure that pupils 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.
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.