

ICT & Online Safety Policy (including acceptable use) 2026 - 2027



Kingsland School

Date of last review:	December 2024
Date of this review:	Feb 2026
Date of next review:	Feb 2027
Comments:	This replaces the policy names ICT & Acceptable use and now encompasses online safety with the Acceptable Use agreement.
Head teacher's Signature:	<i>E. Patel</i>
Review approved by the Governors	Update shared via the Governor Hub on 06.03.2026 For committee (HR) taking place on 10.03.2026

1. Introduction and 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), 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 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 under our disciplinary policy and the staff code of conduct policy.

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](#)
- [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 2022](#)
- [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](#)
- UKCIS 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 which 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 6 for a glossary of cyber security terminology.

4. Unacceptable Use / Breaches of this Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of the user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will carry a possible range of sanctions, consequences or penalties.

In the event of a portable computer being damaged or lost as a result of non-compliance with this policy or as a result of a negligent action, staff may be required to make full or partial contribution towards any reparation/placement at the discretion of the school.

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. This includes connecting any device to the school wi-fi or physically connecting to the network via a data socket.
- 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 (includes emails).
- 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.

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. All requests must be made in writing directly to the School Business Manager.

4.2 Sanctions

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

5. Staff (including Governors, volunteers, 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. This 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 must notify the School Business Manager immediately. Staff who need their access permissions updated or changed, should send the request via email the request to the School Business Manager & ICT Manager.

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. Multi-factor authentication is enabled on all staff email accounts.

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

Staff **must not** share their personal email addresses with parents 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 so that the information is only accessible by the intended recipient. This is done by using the word 'secure' or 'encrypted' anywhere in the subject line of an email.

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 School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents 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 unless in case of emergency (refer to staff handbook)

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**.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, this is with prior authorisation from the Headteacher and subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher or School Business Manager 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 / non break times.
- 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 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.

When using social media in private use; staff must not make reference to pupils, parents/carers of pupils or school staff in work capacity or their role in school. Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

Staff must not engage in personal matters/voice personal opinions relating to members of the school community or school business.

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

5.3 Remote access

We allow members staff to access the school's ICT facilities and materials remotely. Remote access is available to all contracted staff granting them access to the shared files, emails, MIS and CPOMS.

This access is also granted to supply staff when they have worked at the school for 2 weeks and signed the ICT user agreement.

Remote access to MIS systems such as Cpoms and Sims is provided to all staff.

We provide remote learning for pupils and this is detailed in our Virtual Learning Policy.

The School ICT Manager manages the software for both staff and pupil access.

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 take such precautions. They must ensure that the access is restricted at all times including when working from home.

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. This applies to platforms such as Cpoms and Sims.

The school Data Protection Policy is located on our school website.

5.4 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 personnel which includes the ICT Manager and the DSL may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel are advised to raise concerns about monitored activity with the School's Designated Safeguarding lead (DSL) as appropriate.

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.

The Governing Body will regularly review the effectiveness of the school's monitoring and filtering systems.

Schools have a statutory obligation to keep children safe and the use of technology has become a significant component of many safeguarding issues. We aim to reduce the risk to our pupils and ensure that they are not exposed to illegal content.

The issues classified within online safety are considerable but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful on line interaction with other users and
- Conduct: personal online behaviour that increases the likelihood of, or causes harm.

The School utilizes the Council/ZEN internet provision along with Fortinet and Fortiguard Web content filtering. We have been assured by Oldham Council that this provision meets the standards specified in the Keeping Children Safe in Education 2025 Statutory Guidance.

All violations are given a threat score, if these scores are above the normal browsing then an alert is sent to the email address at the LA and at this point it is identified which school the breach has occurred and a report will be generated. The report with the on line safety breach is emailed as an alert the school Safeguarding and ICT Team (including DSL). The email account for this team is monitored daily. This email notifies the team of the IP address and time of breach. The ICT Manager will investigate the breach and identify the pupil to the safeguarding team who will act upon this information accordingly.

The School uses a monitoring system in the ICT suite called Veyon which is used by the teacher delivering the lesson to monitor and identify any breaches to the Acceptable Use Policy

6. Pupils

6.1 Access to ICT facilities

The following ICT facilities are available to pupils:

- Computers and equipment in the Schools teaching and learning areas ONLY under the supervision of staff.
- Pupils are provided with a school email address to allow them access to Microsoft services only, this is not used as a form of communication.
- Pupils are provided with a log in for the school network, this allows them to save their work in a safe, secure area.

6.2 Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026).

All schools have to teach:

- › [Relationships education and health education](#) in primary schools
- › [Relationships and sex education and health education](#) in secondary schools

In **KS3**, pupils will be taught to:

- › Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- › Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- › To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- › How to report a range of concerns

By the **end of secondary school**, pupils will know:

- › Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- › Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- › The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- › Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- › That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime.
- › What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- › About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- › That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong

- › That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- › How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- › That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- › How information and data is generated, collected, shared and used online
- › That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- › That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- › That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND

6.3 Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- › Methods that hackers use to trick people into disclosing personal information
- › Password security
- › Social engineering
- › The risks of removable storage devices (e.g. USBs)
- › Multi-factor authentication
- › How to report a cyber incident or attack
- › How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation

6.4 Search and Deletion

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 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 report the matter to a member of the Senior Leadership team who will will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent.
- 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 (if the pupil refuses to co-operate follow the guidance outlined in the searching, screening and confiscation policy).
- Involve the DSL without delay if they believe that a search has revealed a safeguarding risk.

Members of the Senior Leadership team 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, they should only do so if they reasonably suspect that the data has, 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 the Headteacher / Head of School to decide on a suitable response. If there are images, data or files on the device they reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, consideration will be given as to 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 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) 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 guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy / searching screening and confiscation policy.
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.5 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the school 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 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.

7. Parents

7.1 Access to ICT Facilities and Materials

Parents do not have access to the school's ICT facilities as a matter of course.

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

Where parents 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 play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and via email.

We ask parents to sign the agreement in appendix 2.

7.3 Communicating with parents about pupil activity

Class teachers will let parents know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

7.4 Educating Parents/Carers About Online Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via regular communications from the safeguarding team and or form tutors. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7.5 Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The safeguarding team and teaching staff will discuss cyber-bullying through group discussion and assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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 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 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.

Passwords should not be written down and should not be simple words (particularly obvious things such as surname, the name of a child or a family pet or the word 'password'). Users should note that new accounts are created with simple passwords – this password **MUST** be changed to a new complex password at first log-on and before use.

Staff will not be asked to change their password for any email account, however staff are advised to change their password **every 60 days**, as a matter of good practice.

We require staff to change their passwords to the network **every 42 days**, the network will prompt staff to do this.

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

All users are expected to ensure that their password security is maintained.

Under no circumstances should any user give their password to anyone else or allow anyone else to use their account.

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.

The ICT Manager will generate passwords for pupils who require a password generating.

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.

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 which is located on our school website.

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 School Business Manager & 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 the School Business Manager & 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. Equipment and systems **MUST** always be locked, logged out of or shut down completely at the end of each working day.

Kingsland School;

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Ensures the IT Manager is up to date with services and policies.
- Ensures that storage of all data in school conforms to the Data Protection requirements.
- Has a clear daily back up system and recovery plan for all systems in school.
- Has remote access facilities for ICT staff to manage services such as Sims, CCTV, Website and Active Directory.
- Ensures staff have secure areas on the network to store sensitive documents or photographs. These are not accessible by pupils.

- Request staff to log out of systems when leaving their computer, but also enforce lock out after 10 minutes of idle time.
- All servers are in lockable locations and managed by DBS checked staff.

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, e.g. laptops 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. USB drives are not permitted to be used to store school data.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption and have been checked by the IT Manager.

All staff laptops are encrypted.

9. Use of AI

Artificial Intelligence (AI) technologies are increasingly accessible within educational settings and may support teaching, learning and administrative efficiency when used appropriately. However, AI systems also present safeguarding, data protection, ethical and educational risks which the school must actively manage.

For the purpose of this policy, AI refers to software or online systems capable of generating text, images, audio, video, code or analysis using automated or machine-learning processes.

9.1 Acceptable Educational Use

AI tools may only be used where their use:

- * Supports legitimate educational or operational purposes;
- * Is supervised or authorised by a member of staff;
- * Does not compromise safeguarding, data protection or academic integrity;
- * Complies with all existing school policies including safeguarding, data protection and acceptable use.

Staff must ensure that pupils understand that AI-generated content should support learning and not replace independent thinking or original work.

9.2 Risks Associated with AI Use

The school recognises the following potential dangers associated with AI technologies:

Inaccurate or misleading information: AI-generated responses may contain errors, bias or fabricated information presented as fact.

Academic misconduct: Use of AI to complete assignments or assessments without permission may constitute cheating or plagiarism.

Data protection risks: Entering personal, confidential or sensitive school information into AI systems may result in unauthorised data sharing or storage outside school control.

Safeguarding concerns: AI systems may generate inappropriate, harmful or age-inappropriate content if used without supervision.

Bias and discrimination: AI systems may reflect societal or dataset biases which could reinforce stereotypes or unfair outcomes.

Deepfake and synthetic media risks: AI may be used to create realistic but false images, audio or video which could be used for bullying, harassment, reputational harm or misinformation.

Over-reliance on technology: Excessive dependence on AI tools may negatively impact pupils' critical thinking, creativity and independent learning skills.

9.3 Staff Responsibilities

Staff must:

Not input personal data relating to pupils, staff or parents into AI systems unless explicitly approved and compliant with data protection requirements;

Verify AI-generated information before using it in teaching or communication;

Supervise pupil use of AI tools where permitted;

Report any safeguarding, misinformation or misuse concerns to the Designated Safeguarding Lead (DSL) or ICT Manager.

9.4 Pupil Responsibilities

Pupils must not:

Use AI tools to complete work presented as their own without permission;

Enter personal or school-related confidential information into AI systems;

Use AI to create harmful, offensive, misleading or inappropriate material.

Use AI systems to impersonate staff, pupils or members of the school community.

Misuse of AI technologies will be treated in line with the school behaviour policy and acceptable use procedures.

9.5 Monitoring and Review

The school will regularly review developments in AI technology to ensure safe, ethical and lawful use within education. Guidance and restrictions may be updated as technologies evolve.

10. Protection from cyber attacks

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

The school will:

- Provide information for staff including how to: Check the sender address in an email and respond to a request for bank details, personal information or login details
- 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.

We have the following controls in place:

- Back up of all critical data is carried out daily at 7pm. The system is set to automatically carryout a backup.
- The external hard drives are stored in the ICT Manager's office in a locked drawer.
- The company ESS are responsible for maintaining the security of our management information system (MIS) which is cloud based Sims. We subscribe to Redstor to manage the back up for all Microsoft 365 services.
- The ICT Manager ensures that the firewall in place is switched on.
- There will be additional control measures in the autumn term 2025 to reduce the risk of cyber attacks on the school website using a company by the name of dmarcian.

11. Internet access

The school's wireless internet connection is secure. Filtering is provided by the Local Authority using a third party company (ZEN).

11.2 Parents and visitors

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

This will only be granted if:

- Volunteers are working with the school in an official capacity.
- 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.

12. MIS (Management Information System)

Staff are asked to be aware that the same procedures and rules apply when using systems in school e.g. SIMS, CPOMS. These systems contain personal information relating to pupils; therefore under no circumstances should these applications be left open.

13. Asset Disposal

Details of all school owned hardware will be recorded in the inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item. All redundant equipment that may have held personal data will have the storage media wiped. Alternatively if the storage media has failed it will be physically destroyed. Portable equipment loaned by school staff (for use by staff at home) is disposed of through the same procedure.

14. School Website

Uploading of information is restricted to our website authorisers;

- ICT Manager
- Examinations Officer & Data Analyst

We do not publish photos / images of pupils on our school website. Any request by staff to upload information to the school website are to be sent to the Business Manager via email.

15. CCTV

We have CCTV in the school as part of our site surveillance for staff and pupil safety. We will not reveal any recordings without permission, except where disclosed to the Police or Local Authority as part of an investigation.

15. Related policies & Review

This policy will be reviewed **annually** to take into account any changes in safeguarding to ensure full compliance with protocols and government guidance.

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

- Safeguarding and child protection
- Behaviour Policy
- Staff code of conduct Policy
- Data protection Policy
- Remote education
- Mobile phone policy
-

Reviewed by: C. Emerson & C .Perry
Reviewed by: C. Emerson & C Perry
Reviewed by: C. Emerson & C Perry
Reviewed by: C. Emerson
Reviewed by: C. Emerson & C. Perry
Reviewed by: C. Emerson & C. Perry
Reviewed by: C. Emerson & C .Perry

Date of Review: 05.03.2026
Date of Review: 23rd July 2025
Date of Review: December 2024
Date of Review: October 2023
Date of Review: July 2023
Date of Review: January 2021
Date of Review: October 2018

Appendices:

Appendix 1: Facebook cheat sheet for staff

Appendix 2: Staff– ICT Acceptable Use Agreement

Appendix 3: Pupils – ICT Acceptable Use Agreement

Appendix 4: Glossary of cyber security terminology

Appendix 5 - Filtering Systems

Appendix 6 – Understanding Fortigate Content and Filtering Alerts

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, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your 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. 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 adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent'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'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 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 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

Staff– ICT Acceptable Use Agreement

Staff Name:

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that staff have good access to digital technologies to enhance learning opportunities for our students and in return staff will be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own professional and personal safety:

- I understand that the school will monitor my use of the systems, email and other devices and digital communications.
- I understand that the rules set out in this agreement also apply to the use of the School ICT systems (e.g laptops, email) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will immediately report any inappropriate or harmful material or messages I become aware of to a member of the Senior Leadership Team.
- I will read and be familiar with the ICT & Acceptable Use Policy.

I will be professional in my communications and actions when using School ICT systems

- I will not access, copy, remove or otherwise alter any other users's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take / or publish images of others I will do so with their permission in accordance with the school policy. I will not use my personal equipment to record these images.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will only communication with young people and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- If the data on any device is breached I will report it to the Business Manager immediately.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- When I use personal / external devices e.g. laptop, tablets I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open attachment to emails unless the source is known and trusted due to the risk of the attachment containing viruses or other harmful programmes.
- I understand the importance of regularly backing up my work.
- I will not to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography) or inappropriate or may cause harm or distress to others.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy.
- I will immediately report any damage or faults involving equipment or software.

I understand that I am responsible for my actions in and out of school.

I understand that the Acceptable Use Agreement applies not only to my work and use of ICT equipment in school but also applies to my use of school ICT systems and equipment out of school.

I understand that if I fail to comply with this Acceptable Use Agreement I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the Police.

I have read and understand the ICT & Internet Acceptable Use Policy and Agreement.

Staff Name: _____

Signed: _____

Date: _____



Kingsland School

Pupils – ICT Acceptable Use Agreement

Name of Pupil:

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) or any other non-educational purpose, unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use USB devices in school unless I have written permission from the Headteacher or Business Manager. I understand that, if I do wish to use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will not attempt to use social media sites.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Responsible Internet Use (Information to parents/carers)

As part of your child's curriculum and the development of ICT skills, Kingsland School is providing supervised access to the Internet. We believe that the effective use of the World Wide Web is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school. If you wish to see a copy of the school's E-Safety & Acceptable Use Policy' this is available on the school website.

Although there are concerns about students potentially having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed

through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Please be aware that if any safeguarding issues are identified including possible attempts around radicalisation, staff at Kingsland School will follow the procedures as outlined in the Child Protection and Safeguarding Policy.

Rules for Responsible Internet Use

The computer system is owned by the school. This Acceptable Use Agreement helps to protect pupils, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the pupil's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of unauthorised chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the head teacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I hereby confirm that I have read and fully understand the terms and conditions of the ICT & Internet Acceptable Use Agreement.

Print full Name of Pupil: _____

Signature of Pupil: _____ Date: _____

Print full Name of Parent/carer: _____

Signature of Parent/carer: _____ Date: _____

Appendix 4: 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.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
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 5

Filtering System

All violations of policies are given a threat score, if the scores are above normal browsing then a report is generated which is sent to the email address live.iib@oldham.gov.uk. This information is then sent via email to the DSL and the Safeguarding Team.

What categories are blocked by default?

1. Security Risk

Malicious Websites

Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.

Phishing

Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.

Spam URLs

Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.

2. Bandwidth

Streaming Media and Download

Websites that allow the downloading of MP3 or other multimedia files.

Peer-to-peer File Sharing

Websites that allow users to share files and data storage between each other.

3. Potentially liable

Drug Abuse

Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.

Hacking

Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.

Illegal or Unethical

Websites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc.

Discrimination

Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.

Explicit Violence

This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.

Extremist Groups

Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.

Proxy Avoidance

Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers.

Plagiarism

Websites that provide, distribute or sell school essays, projects, or diplomas.

Child Abuse

Websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at <http://www.iwf.org.uk/>.

4. Adult / Mature content**Other Adult Materials**

Mature content websites (18+ years and over) that feature or promote sexuality, strip clubs, sex shops, etc. excluding sex education, without the intent to sexually arouse.

Gambling

Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.

Nudity and Risque

Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse.

Pornography

Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.

Weapons (Sales)

Websites that feature the legal promotion or sale of weapons such as hand guns, knives, rifles, explosives, etc.

Marijuana

Sites that provide information about or promote the cultivation, preparation, or use of marijuana.

Alcohol

Websites which legally promote or sell alcohol products and accessories.

Tobacco

Websites which legally promote or sell tobacco products and accessories.

5. General interest – personal**Instant Messaging**

Sites that allow users to communicate in real-time over the Internet.

Domain Parking

Sites that simply are place holders of domains without meaningful content.