Online Safety Policy

Leytonstone
SCHOOL

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools - GOV.UK (www.gov.uk)
- Preventing bullying - GOV.UK (www.gov.uk) and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk)

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 (legislation.gov.uk) and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Maintained schools and academies that follow the National Curriculum insert:

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety with the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Fiona Sinclair

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and Deputy DSL's are set out in safeguarding policy document.

The Designated Safeguarding Lead is:

Marta Hotez mhotez@leytonstoneschool.org

The Deputy DSLs are:

Paul Hunt phunt@leytonstoneschool.org

Innes Weir iweir@leytonstoneschool.org

You may also email safeguarding@leytonstoneschool.org

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify the Headteacher or the DSL of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Hot Topic | Childnet
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect NoBody campaign - GOV.UK (www.gov.uk)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

In **Key Stage 3**, 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 **Key Stage 4** 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:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or social media accounts. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

Concerns or queries about this policy can be raised with the DSL or the Headteacher.

6. Cyber-bullying

6.1 Definition

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 one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 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 are encouraged 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. Form tutors will discuss cyber-bullying with their tutor groups.

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 Safeguarding training, including online safety training, 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 so that 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring one mobile devices into school, but are not permitted to use them during the school day or on the school site. Students are expected to place their phones (switched off) in their bags.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 15 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol), along with MFA (Multi Factor Authentication) in all cases.
- Locking the device when not in use or making sure the device auto locks if left inactive for a period of time (10 minutes)
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from their SLT Line Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff briefings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in our electronic safeguarding recording system.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the Governing Body.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Keeping Children Safe in Education
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet Acceptable Use Policy
- Cyber Security Policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • 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 • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will abide by the school's behaviour policy with regard to mobile phones and electronic devices • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's 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 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Acceptable use of ICT, the internet and social media: STAFF

It is important that you are fully aware of the safety rules and procedures which regulate your use of our ICT resources, including ICT devices and the internet. At Leytonstone School we encourage and allow all staff access to our curriculum network and the internet enabling you to use vast resources in support of research and education.
We insist that these facilities are used for educational purposes and in an appropriate manner. You are responsible for your behaviour and communication. Any breach of the rules will be considered a disciplinary matter.

- I will not allow pupils to access sensitive data and information by not responsibly password-protecting and securing my workstation/ laptop.
- I will not violate any laws such as: Accessing or transmitting any kind, obscene, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
- I will not engage in criminal activities that can be punished under law.
- I will not obtain and/or use anonymous email sites; spamming; spreading viruses.
- I will not use abusive, or impolite language; threatening, harassing, or make damaging or false statements about others or access, transmit, or download offensive materials.
- I will not delete, copy, modify, or forge other users' names, emails, files, or data; disguise my identity, impersonate other users, or send anonymous emails.
- I will not damage computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
- I will not use any school computer to pursue "hacking," internal or external to the school, or attempt to access information protected by privacy laws.
- I will not access, transmit or download "chain letters".
- I will not use another's account password(s) and user identifier(s).
- I will not disclose anyone's password to others or allowing them to use another's account(s).
- I will not use personal devices in school to take or transfer images of pupils and/or staff
- I will not record conversations without the consent of all parties involved
- I will not communicate with and/or befriend pupils on roll via social media.
- I will not communicateating with pupils on roll via non-school email accounts.
- I will not use the internet for personal financial gain, personal advertising, promotion, or financial gain.

I have read, understand, and agree to follow the Acceptable Use of ICT Policy of Leytonstone School
Date:
Name:
Signature:

Guidance to consider (source NEU 2019):
The nature of teaching and working in education means that school staff need to be particularly aware of their online reputation, including information posted about them by others. While the NEU does not advise members against using social media for personal use, it does advise them to think carefully about the way they use these technologies.

There have been cases of school employees being subject to disciplinary action because of inappropriate postings online.

Below is NEU advice for school staff on how to stay safe online and when using technology and social media:

- Review your privacy settings, and ensure that they are sufficiently robust. Sites such as Facebook allow you to view your page
- as different groups of people, e.g. friends, non-friends.
- Privacy tools that are available on many social media sites include: customising who can see your posts; controlling who can
- contact you and make 'friend' requests; keeping your location private; and approving tags before they are published.
- Discuss expectations around tagging posts with friends and family. For instance, you may prefer to not be tagged in any posts
- on social media.
- Regularly search your name in search engines and social media sites to check what information there is on the internet about
- you. It is standard practice for employers to search prospective employees online, so search yourself online when applying for
- any posts. When searching, check variations of your name and even nicknames.
- If offensive or hurtful information is posted about you online, for instance, by a pupil or parent, never retaliate to the message.
- There have been cases where school staff have been disciplined by their employer for responding to posts online, even where
- they were not the instigator. Instead, make copies of all offensive content, including screenshots and URLs, and take them to
- your employer. Your employer must take action on cyberbullying in the same way as it would face-to-face bullying.
- If offensive material has been posted about you online, you can use the reporting procedures of the site involved to get the
- material taken down. More information on how to do this is available in the NEU self-help briefing on cyberbullying.

- Make sure you have familiarised yourself with your employer's IT 'acceptable use' policy and abide by the requirements of this
- policy. For instance, if you access personal email and social media accounts when connected to the employer's Wi-Fi network,
- these may be subject to the school's internet policy which is likely to include monitoring and surveillance.
- Only use work equipment and email for work uses – and do not let anyone else, including colleagues and family members, use
- them.
- Ensure all of your devices, including work ones, are password protected. Do not give your password to anyone else and do not
- leave your screen unlocked if you move away from the device.
- Do not befriend any current pupils on social media – it is likely to be in breach of your employer's policies. If pupils are
- constantly attempting to 'friend' you on social media, report this to your employer.
- While former pupils may not be covered by your employer's policy, NEU advice is to very carefully consider the implications of befriending former pupils, especially as they may have friends, siblings or connections to current pupils. Similarly, there are potential implications of befriending parents of pupils on social media – even if they are also a colleague. Therefore, it is recommended that NEU members do not friend former pupils or parents on social media. If you do decide to do this, let your employer know.
- Keep your personal phone number private and do not share with pupils or parents. If it is necessary to use a mobile phone to contact parents, e.g. during a school trip, your employer must provide one.
- Be aware that your employer will be able to check your usage and data, including location history, on any device they provide you for work purposes.
- When using social media, before posting or commenting on items, consider whether you would be happy for your employer, colleagues, pupils and parents to see it. If you wouldn't want them to, then don't post it online.
- Never criticise your school, employer, pupils or parents online.

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No** **(add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: IT Filtering and Monitoring

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Content filtering is provided by LGFL and their Webscreen software, local monitoring and safeguarding is provided by Impero.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Systems Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems as well as list of the defined filters for user groups.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme, students also sign the "ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS" agreement (appendix 1). They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness briefings/updates etc.

Changes to the Filtering System

Staff wishing to request a change to the filtering system should contact the ICT Manager with the details of the URL they are wishing to access, giving clear educational reasons as to why they think the URL should be allowed, which users should be allowed access, the length of time access will be required.

The grounds on which requests may be allowed or denied will be in accordance with the schools Online Safety Policy. Please note there should be strong educational reasons for changes to be agreed.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement. Monitoring will take place as follows:

- Students activity on the ICT Systems as monitored by Impero will be processed and a report sent to the DSL, any concerns will be processed in accordance with the schools Safeguarding Procedures.

Appendix 5: Password Security Policy

Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's Data Protection Policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

Responsibilities

- The management of the password security policy, along with enabling of Multi Factor Authentication (MFA) will be the responsibility of IT Systems Manager
- All users (adults and young people) will have responsibility for the security of their own username and password, users must not give their username / password to anybody else. Users must not allow other users to access or use the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- New and Replacement staff passwords can be allocated by the IT Team, the request for a password change needs to come directly from the member of staff concerned. Once staff have logged onto their accounts, they need to ensure that they change their passwords via the log in screen. The Headteacher, Deputy Heads or Business Manager can request a password change for another member of staff's account should the need arise. This request needs to be documented with a brief description of why the request was made.
- Student Passwords for new users, and replacement passwords for existing student users can be allocated by the IT Team. Students do not have the facility to change their own passwords, this function has been restricted.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or online safety lessons/assemblies
- Form Tutor time
- Through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the IT Systems Manager and will be reviewed annually.
All users will be provided with a username and password by the IT Team who will keep an up to date record of users and their usernames. Staff users will be required to change their passwords every 60 days.
The following rules apply to the use of passwords:

- Staff account must have Multi Factor Authentication enabled where applicable
- The password should be a minimum of 15 characters long – Staff
- The password should be a minimum of 6 characters long / 8 for Google – Students
- Passwords must include a mix of alphanumeric characters – Staff
- Accounts will be "locked out" following five successive incorrect log-on attempts – All users
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed – All users
- Requests for password changes should only be issued to the user directly unless a request has been made by the Headteacher, Deputy Heads or the Business Manager with clear reason for the request.

The "master / administrator" passwords for the school ICT system, used by the IT Systems Manager and Technicians will be available to the Headteacher and Business Manager. The Headteacher will also be given a master / administrator' username and password of their own to access to the ICT System including the Server.

Audit / Monitoring / Reporting / Review

The ICT Manager will ensure that full records are kept of:

- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords.
Local Authority Auditors also have the right of access to passwords for audit investigation purposes.
User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

This policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.