RUSSELLS HALL PRIMARY SCHOOL

School Key Policy for 2026-2027

Online Safety Policy

September 2026

Document to be read in conjunction with ***other key school policies (listed within document)***

Approved by:	John Cook, Chair of Governors	**Date:** October 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 6
5. Educating parents about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 8
9. Staff using work devices outside school 8
10. How the school will respond to issues of misuse 8
11. Training 9
12. Monitoring arrangements 9
13. Links with other policies 9
Appendix 1: Pupils acceptable use agreement (all pupils and parents/carers) 10
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 12
Appendix 3: Password Security Policy 16

---

1. Aims

Russells Hall Primary 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
- Preventing and tackling bullying 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 protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 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. The policy also reflects the Children's Wellbeing and Schools Act 2026.

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Personnel committee are the governors that oversee online safety.

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 deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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, Online Learning Lead, ICT manager (RM) and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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
- 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 daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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.

3.5 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 (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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 a member of staff or the headteacher 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 (appendix 1)

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 - Childnet International

- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

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:

The text below is taken from the National Curriculum computing programmes of study.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The text below is taken from the Relationships education and health education in primary schools

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

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

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 ParentHub. This policy will also be shared with parents.

Where applicable, 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 and/or the DSL.

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

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. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, Russells Hall Primary School 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.

Russells Hall Primary 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. 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, Computing 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).

When appropriate, Russells Hall 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, Russells Hall will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, Russells Hall will use all reasonable endeavours to ensure the incident is contained.

The DSL and/or deputy 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

As a primary school, children are not permitted to bring personal electronic devices into school without prior agreement from parents or carers, in exceptional circumstances (see section 8).

Under the Education and Inspections Act 2006 (enhanced by the Education Act 2011), Russells Hall Primary School is entitled 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. However, Russells Hall would only ever do this in partnership with parents.

7. Acceptable use of the Internet in school

At Russells Hall, 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 1-2). 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. This is monitored 24/7, 365 days a year by E-safe.

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

8. Pupils using mobile devices in school

Pupils at Russells Hall Primary School are not permitted to bring a mobile device into school. At the request of a parent or carer, a child may be allowed to bring a mobile phone into school for the expressed purpose of walking home alone. In this instance, the mobile phone will be handed into the school office on arrival where it will be kept until the end of the school day.

9. Staff using work devices outside school

At Russells Hall, 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 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) (see appendix 3)
- Using school's OneDrive opposed to external hard drives. In the exceptionally rare event where the use of portable hard drives is unavoidable, ensuring their hard drive is encrypted.
- Making sure the device locks if left inactive for a period of time
- 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 the Online Learning Lead or ICT 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 behaviour policy and acceptable use agreement. 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

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, staff meetings and training days).

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 child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident will be logged on CPOMS.

This policy will be reviewed every year by the Designated Safeguarding Lead and the Online Learning Lead. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy and Written Statement of Behaviour Principles
- Anti-bullying policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement

Appendix 1: Pupils acceptable use agreement (all pupils and parents/carers)

Russells Hall Primary

Rules for Responsible Internet Use

For Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff, so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g. Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network, I will check with my teacher to see if it is possible.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.



Your child will use the internet in school unless you specifically request that they do not. If this is the case, please return the slip below.

✂……

Only return this section if you <u>do not</u> want your child to use the internet.

I do not want my child _____to access the internet.

Class:_____

Signed _____Parent/Carer

PRINT NAME……

Dated: …….

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

Russells Hall Primary

Staff Acceptable Use Agreement

Rules for Responsible Internet use

This policy applies to all adult users of the school's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- If you download any image, text or material check if it is copyright protected. If it is then following the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.

- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.
Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply: -

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. X

When using school approved social networking sites, the following statements apply: -

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @<schoolname>. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the current Data Protection Act.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must: -

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the current Data Protection Act and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Dated October 2026

Appendix 3: Password Security Policy

Russells Hall Primary
School Password Security Policy

This policy is in conjunction with school's on-line safety policy and accordance with Data Protection Law and other related government legislation.

Introduction
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 personal data protection policy.
- Logs are maintained of access by users and of their actions while users of the system by e-Safe Systems Ltd.
- Safe and secure username / password system is essential if the above is to be established and will apply to all ICT systems within school, including email.

Responsibilities
The management of the password security policy will be the responsibility of Headteacher and School Business Manager.

All users (adults and young people) will have responsibility for the security of their username, password and must not allow other users to access school's systems using their log on details and must immediately report any suspicion or evidence that there has been any breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the school admin team.

Password security consists of the following:

- Enforce password history - stops reusing old ones.
- Maximum password age – 240 days (staff and pupils will be asked to change their password)
- Minimum password age - 1 day
- Minimum password length – minimum of 10 characters. Need to avoid dictionary words or people's names, even with numbers and special characters to disguise. (Hackers with over a million dictionary combination database can crack those in seconds).
- Password must meet complexity requirements.
- Account lockout – 8 failed attempts locks the account for 30 minutes.

Pupils using ICT in school

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

- In ICT and / or e-safety lessons.
- Through the use of posters placed in classrooms and around school.

Visitors / Contractors / Members of the wider community

Visitors, contractors, and members of the wider community will be made aware of the school's password policy and in accordance with school's e-safety policy and with the Data Protection Law and other related government legislation.

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 E-Safety Co-ordinator.

Audit / Monitoring / Reporting / Review
The Headteacher/School Business Manager will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

A strong password will ... include a range of characters

- Upper case and lower case letters
- Numbers
- Punctuation marks
- Other symbols
- Minimum of 10 characters
- Include a range of characters, such as:
- Not contain dictionary words, where possible
- Not include simple substitutions of characters, e.g. "p4$$w0rd"
- Not include patterns derived from the keyboard layout, e.g. "qwerty"
- You should also avoid using obvious choices of passwords, such as the name of your child or pet, as someone could find such information elsewhere.

Security incidents related to this policy

School has a responsibility for protecting the personal information of its pupils and staff in accordance with GDPR.

……..The Information Commissioner's Office recommends not saving passwords for any system used in schools. The representative explained if a password is saved, for example directly into a system, any individual can access the system using another's name or username.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

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 regularly reviewed in response to any changes in guidance and evidence gained from the DfE and the Local Authority.

Appendix: Artificial Intelligence (AI) – Guidance for Safe and Appropriate Use

This appendix outlines the school's approach to the safe and responsible use of Artificial Intelligence (AI) technologies. As AI becomes increasingly present in education and everyday life, it is essential that pupils, staff, and governors understand the opportunities and risks it presents, particularly in relation to **safeguarding, data protection, and digital literacy**.

1. Purpose and Scope

This guidance applies to all members of the school community, including staff, pupils, and governors, and covers any interaction with AI tools or services, whether within the school environment or beyond.

AI includes (but is not limited to):

- Chatbots or conversational tools (e.g. virtual assistants).
- Image and video generation.
- Automated marking or content creation tools.
- Data-driven decision-making systems.

2. Guiding Principles for AI Use in School

- AI should be used to **support learning**, creativity, and critical thinking, not to replace human judgement or diminish educational value.
- AI tools must be used in ways that **respect privacy**, promote **online safety**, and align with the school's **safeguarding and data protection** policies.
- Staff and students should develop an understanding of AI's **limitations**, including its potential for **bias, misinformation, or misuse**.

3. Safeguarding Considerations

- AI-generated content may not always be age-appropriate, accurate, or safe. Pupils must be **supervised** when interacting with any AI tool.
- Any concerns arising from pupil use of AI — including access to inappropriate material or use of AI to deceive, harass, or bully — will be treated as a **safeguarding issue**.
- Staff should model safe, ethical AI use and **report any misuse** of AI in accordance with the school's online safety procedures.

4. Data Protection and Privacy

- AI tools must not be used to process or share **personal data** of pupils, staff, or parents unless authorised and compliant with GDPR.
- Staff and pupils must avoid entering identifiable information into AI platforms, particularly those outside the school's control or hosted overseas.

- Where AI is used to support school operations (e.g. administration, learning analytics), a **data protection impact assessment (DPIA)** may be required.

5. Staff Expectations

- Staff may use AI to assist with planning, assessment, or administrative tasks, provided:
    - It does not compromise **accuracy, fairness, or professional judgement**.
    - Pupil data or confidential information is not shared with third-party AI systems.
    - Any AI-generated material is **reviewed and edited** before being used in teaching or communication.
- Staff should help pupils develop **critical thinking** skills to understand how AI works and how to evaluate AI-generated information.

6. Pupil Expectations

- Pupils may be introduced to AI concepts in the computing curriculum, in line with the **Teach Computing** framework.
- Any direct use of AI tools by pupils must be:
    - **Age-appropriate** and under staff guidance.
    - Used for **educational purposes** only.
    - Accompanied by discussion about **safe, ethical, and fair use**.
- Pupils must never use AI tools to:
    - Impersonate others.
    - Plagiarise work or avoid independent learning.
    - Generate harmful, misleading, or inappropriate content.

7. Monitoring and Review

- AI-related activity within the school network is subject to the same **Smoothwall filtering and monitoring** as all digital activity.
- This appendix will be reviewed annually, or sooner if AI use in education significantly changes or if new risks are identified.

Further Support and Resources

- Online Safety Lead / DSL: Sarah Hawker / Helen Houlston
- DPO (Data Protection Officer): YourIG Data Protection Officer Service, Dudley MBC, The Council House, Dudley, DY1 1HF; YourGDPOService@dudley.gov.uk; 01384815607
- National Online Safety: https://nationalonlinesafety.com/
- UK Safer Internet Centre: https://www.saferinternet.org.uk/
- ICO guidance on AI and data protection: https://ico.org.uk