



## Acceptable Use of ICT Policy for Pupils with School Provided Home Learning Device - September 2020 – Proposed changes 2025

---

### 1. Introduction

- 1.1 This acceptable use policy identifies the responsibility of school pupils and provides helpful information and guidance for everyday life as well as setting out the expectations for using digital equipment in school.

### 2. Scope

- 2.1 This Acceptable Use Policy outlines the standards of conduct that every pupil must adhere to when using school digital equipment or when using personally-owned devices for school purposes. Following these guidelines and behaviors will ensure that pupils meet the standards for use of technology set out by their school. The purpose of this is to protect children when online and to protect the School's network and equipment.

### 3. Staying Safe Online

- 3.1 It is important that pupils know how to keep safe online and know who to report to. If a pupil has any concerns, they should speak to someone they trust immediately such as a teacher, Parent, Carer. Pupils can also report someone who is threatening or blackmailing them online to the police through CEOP <https://www.ceop.police.uk/ceop-reporting/>
- 3.2 Access to free advice and support for pupils suffering bullying online <https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/bullying-social-media/>.
- 3.3 Access to advice to help for pupils to keep safe and to know what to do when things go wrong including information on: what are the risks, tips to stay safe online, keeping your information secure and how to spot fake news. <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/>
- 3.4 Further free advice on safe internet use for parents and young people is available from the following source: [CEOP Education](#)
- 3.5 Here are some guidelines to help ensure your safety online: -
- Think carefully before posting, do not share anything you would not want your Parent, Carers, teachers or even future employers seeing. Once it has been posted, it is



available on the internet of people to share or take screenshots. It is very difficult to delete anything permanently.

- Do not share your personal details or details of others. Personal details include: addresses, phone numbers, full names, your school, and date of birth.
- Watch out for phishing and scams. People can try to trick you into giving them your personal information. Do not click on email links or attachments of unknown senders. Do not enter your details from an email link, use the actual website or app so you know it is genuine.
- Be careful who you are talking to. Never give out personal information to someone you have met online. People are not always who they say they are. You should never agree to meet in real life someone you meet online.
- Never give out your password as others can log in pretending they are you and use inappropriate behavior or steal your information. Pick a strong, easy to remember password.

## Key Principles and Rules

### 4. Access to the Internet

- 4.1 Internet access allows pupils an opening to a wealth of information, knowledge and educational resources, increasing opportunities for learning in and beyond the classroom. We provide pupils with access to the internet, including web sites, resources, content, apps and online tools.
- 4.2 When in School pupil access to the internet is filtered to meet school and local authority policies. This is not the case when accessing the internet from a home network. No access to internet is 100% risk-free, pupils should alert their teacher/Parent/Carer should they believe that the content they are viewing is inappropriate. Pupils must not try to get around any filters when browsing online.

### 5. E-Mail Communication

- 5.1 We provide pupils with glow e-mail accounts for the purpose of education-related communication. School e-mail should be used with care and respect. Pupils are expected to communicate with the same appropriate, safe, and courteous conduct online as offline. E-mail is not guaranteed to be private and may be monitored.

### 6. Use of school-owned devices



6.1 Pupils may be provided with a mobile device to support their learning. Pupils must ensure they look after these carefully. Any loss, damage or failure should be reported to their teacher straight away. You may be liable for any damage resulting from negligence or mistreatment.

6.2 Pupils will be expected to: -

- Always look after the device carefully.
- Remember to save any local files to OneDrive on Glow before you close the device down.
- Only use applications on the device that the school has agreed can be used in the lessons.
- Only use the device to record audio or video clips with the clear and explicit permission of everyone involved in the recording and with direction from their teacher.
- Only stream video or music as guided by the teacher.
- Never access inappropriate content on the device.
- Report to your Parent/Carer should any inappropriate material appear on the screen.
- Not download social media apps e.g. X/Twitter, Facebook, Instagram, Snapchat, Messenger, etc. as these are not permitted.
- Not remove any security markings and not allow it to be subject to graffiti.
- Immediately report any damage, loss or theft to their Parent/Carer.
- Report any technical problems to their teacher.

6.3 Parents / Carers should: -

- Ensure that the pupil cares for and respects their device.
- Regularly check the plug and cable for wear and damage. If damaged stop using the device and return it to the school for repair. Immediately report any loss or theft which happens out of school to a member of school staff.
- Please report any breakages and/or technical issues to a member of school staff.
- Ensure that the device is used solely by the pupil that the school has given it to.
- Monitor the use of the device on the internet at home, to ensure that only appropriate websites are accessed, and only appropriate apps are installed.
- Should any inappropriate material appear on the screen please report this to a member of school staff.

## **7. Digital Citizenship and Internet Etiquette**

Pupils should: -

- Be respectful - Pupils should always use the internet, network resources, and online sites in a polite and respectful manner by treating others how they would like to be treated.



- Privacy – Pupils should not provide personal information belonging to themselves or others.
- Digital Footprint – Is information pupils leave behind as they use the internet. A footprint can include comments made on social media, video calls, websites visited and email records. It is part of a pupil's online history that's can sometimes be shared and spread in ways that were never intended. It can also leave a permanent trail which can potentially be seen by parents, teachers, employers, further education and police.
- Be responsible - Whether a pupil accesses school learning from home or school, their responsibility as a pupil remains the same.
- Be Appropriate - Inappropriate behavior towards others will not be tolerated and will have consequences.

## 8. Downloading, Copyright and Plagiarism

- 8.1 For the security of the school network, downloading files such as images, videos, documents, etc. should only be with the agreement of a pupil's teacher and only from trustworthy sites. Viruses can cause serious harm to the security of the School's network and that of others. Pupils must not download offensive material. Viruses are often spread through internet downloads or circulated as attachments to emails. If a pupil thinks or suspects that an attachment, or other downloadable material, might contain a virus, they must speak to their teacher before opening the attachment or downloading the material.
- 8.2 Pupils must make sure they have permission from the copyright owner to copy or adapt material such as music, images, text, icons audio etc. on the internet. It is advised to look for copyright free, music and videos. If uncertain on the copyright, check with the owner of the site on which the material is held.
- 8.3 Plagiarism is the copying or using other people's work and then and passing them off as your own, for example, copying text from a website and using it as your own for a homework assignment. Pupils should not copy or take credit for someone else's work. To avoid plagiarism, give credit to the original author and either add quotations (if word for word) or put their ideas into your own words (paraphrasing). Ask your teacher if you are unsure.
- 8.4 Generative AI tools frequently use large data sets of existing content to draw upon when generating 'new' content. Learners should be aware that claiming content generated



through AI tools as their own work may be perceived by some assessors as a form of plagiarism and treated in the same manner.

- 8.5 Plagiarism is not worth it! The Scottish Qualification Authority treats plagiarism extremely seriously. If plagiarism is identified, a pupil could receive one of the of the following penalties:
- Cancellation of all of the pupil's subject entries for that year
  - Cancellation of the entry of the subject/level concerned
  - The piece of work will be awarded zero marks
  - A warning will be issued

## **9. Monitoring and Limitation of Liability**

- 9.1 Accessing the school internet with a school device, a device lent to a pupil or a pupil's own device for school Wi-Fi access is automatically recorded and may be monitored by Fife Council. This monitoring is for the prevention and detection of unauthorised use of the Council's communication systems. Authorised staff can access logs of websites previously visited by pupils. Such reporting is not undertaken routinely but will be available in the event of an investigation into inappropriate use of the internet or other online tools.
- 9.2 On leaving school, pupils must ensure that all digital equipment provided is returned and in good condition.
- 9.3 Working with others is an essential part of learning. We may provide pupils with access to managed educational web sites, applications or tools that allow them to communicate, collaborate, share, and send messages to other users within the secure application. We may monitor pupil posts, chats, sharing, and messaging. In school or out with school. pupils should be careful not to share personal information that could identify themselves such as their address, email address or mobile number.
- 9.4 While Fife Council includes internet filtration and other safety and security measures, they cannot guarantee to be 100% effective. We will not be responsible, financially or otherwise, for unauthorised transactions conducted over the network.
- 9.5 We will not be responsible for damage or harm to your own devices. Pupils should not share or lend their device to other pupils. A sturdy case is recommended for any devices brought into school.



## ICT Acceptable Use Policy for Pupils

### Pupil Summary Sheet

#### 1. Introduction

- 1.1 Working with others is an essential part of learning. We may provide pupils with access to managed educational web sites, applications or tools that allow them to communicate, work with others, share, and send messages to other users within the application. There are many benefits to you in using the digital facilities in your school but this right carries with it corresponding responsibilities on your part.
- 1.2 This policy sets out the expectations of the Education Service in relation to digital technology and online use within schools. It intends to ensure safe and responsible practice and to clarify respective responsibilities. To gain access to the network and the Internet, including e-mail facilities you are required to:
- Read this policy.
  - Sign the Agreement Form provided
  - Ensure that your Parent/Carer also signs the Agreement Form.
- 1.3 By signing the Agreement Form and returning it to the school, you are indicating that you understand and accept the rules and procedures outlined in the Policy.

#### 2. Network Use

- 2.1 When using school digital equipment and services at school or at home, **I will:**
- only use the applications and network facilities you have been given permission to access.
  - only use your own username and password and do not share them with others.
  - always log off at the end of each session.
  - only store schoolwork in the storage area provided by your school.
  - not attempt to change network settings or bypass the network security systems in any way.
  - understand that the Network Administrator can view any files stored on the system and that regular checks are made.

#### 3. Internet Use

- 3.1 When using school digital equipment and services at school at home, **I will:**



- Use Internet access for school-related activities and research only.
- Only access the internet with permission from your teacher.
- Not provide personal details online and never arrange to meet someone. If meetings are required as part of your education these will be organised by your teacher.
- Not stream video in school without my teacher's knowledge.
- Follow internet safety guidance at home where the school filters do not apply.
- Tell your teacher or other staff member if you see threatening/bullying, inappropriate, or harmful content (images, video, messages, emails or posts) online.
- Not attempt to bypass the internet filtering system by use of proxy servers or any other means.
- Not use text chat facilities for off-topic discussion. Any inappropriate comments made can be traced back to individual users.
- Inform your teacher at once if you accidentally access unsuitable material.
- Not search for inappropriate material.
- Only use email, social media or messaging systems that have been provided by the school for education purposes.
- Not use bulletin boards, forums or conferences unless you have permission to access them and only do so for educational use.
- Not download or use copyright materials without permission of the copyright holder.
- Not access social networking sites (e.g. X/Twitter or Facebook), instead you should be using glow.
- Never send messages which could cause offence or upset to anyone (known as Cyberbullying)
- Be polite when online. Never use bad language
- Not open email attachments unless you are sure what they contain. If in doubt, ask your teacher.
- Not send or forward emails containing explicit, racist or offensive material or images.
- Be aware that the Network Administrator regularly checks the usage of email and misuse of this facility is likely to result in the withdrawal of your email account.
- Switch ringers/notifications to silent whilst in school and will not respond to calls or messages.
- Mute my microphone when I am not contributing to ensure background interference is minimized if taking part in an online teacher lesson.

Any exceptions to these rules will be decided by the school's senior management in consultation with the Fife Education Service.

## 4. Unacceptable Use

4.1 When using school digital equipment and services at school or home, **you will not:**

- Use it in a way that could be personally or physically harmful to yourself or others.
- Search for inappropriate images or content.



- Bully, harass, or be disrespectful towards staff or other pupils.
- Try to find ways to bypass the Council's security and safety measures and filtering tools.
- Send spam or chain mail.
- Copy content you find online without saying where you got it from.
- Post information that could identify yourself or others.
- Publish, post or release information that is confidential or private.
- Agree to meet in real life someone you have met online.
- Use language online that would not be allowed in the classroom.
- Use equipment and services to do things that are illegal or to search for information on illegal activities.
- Attempt to hack or access sites, servers, accounts, or content that you are not allowed to access.

Note: This is not intended to be an exhaustive list. Users should use their own judgement when using technologies.

## 5. Consequences

### 5.1 Please note that failure to comply with the policy on Acceptable Use could result in one or more of the following actions being taken:

1. Temporary or permanent withdrawal of access to the Internet.
2. A letter sent home about the rule/s you have broken.
3. Removal of an allocated home learning device.
4. Restriction on your use of the school digital facilities.
5. Any other action decided by the Headteacher.