

Hautlieu School
Mobile Phone Policy

Author – Claire Jackson

Agreed by Staff – June 2025

Agreed by Governors - July 2025

Revised with Minor Amendments: July 2026
--

To be reviewed: July 2027

Contents

1. Introduction and aims.....	2
2. Roles and responsibilities.....	2
3. Use of mobile phones by staff	2
4. Use of mobile phones by students.....	3
6. Loss, theft or damage.....	5
7. Monitoring and review	5
8. Links to UNCRC – Rights Respecting Schools	5
9. Useful Links.....	6
10. Links to other policies	6
11. Appendices.....	7

1. Introduction and aims

In line with the instructions provided by the Minister for Education and Lifelong Learning in June 2025, Hautlieu aims to foster digital confidence, set healthy boundaries and build the resilience of students to thrive on-line and off-line.

Our policy aims to:

- Set clear guidelines for the use of mobile phones for Key Stage 4 and Key Stage 5 students, staff, parents/carers, visitors and volunteers
- Support Hautlieu School's other policies; Safeguarding, Counter-Bullying and Behaviour for Learning

Note: throughout this policy, 'mobile phones' refers to mobile phones and similar devices.

2. Roles and responsibilities

2.1 Staff

All staff (including teachers, support staff and supply staff) are responsible for consistently enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The Deputy Headteacher for Student Progress and Staff Development is responsible for monitoring the policy annually, reviewing it, and holding staff and Students accountable for its implementation.

3. Use of mobile phones by staff

3.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) should not be using their personal mobile phone, while students are present/during contact time unless it is to use the Authenticator App to allow for Two Factor Authentication of system logins or for contacting the Exams Officer when invigilating an examination. Use of personal mobile phones should be restricted to non-contact time.

There may be circumstances in which it's appropriate for a member of staff to have use of their mobile phone during contact time for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The member of staff must seek permission from the Headteacher who will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number 01534 736242 as a point of emergency contact.

3.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Bard).

For more detailed guidance, please refer to CYPES ICT Acceptable Use Policy for staff. (Appendix 1)

3.3 Safeguarding

Staff must inform the school of any prior relationship with a student. They must not give their personal contact details to parents/carers or students unless they have declared this prior relationship. This includes connecting through social media and messaging apps.

Staff must avoid publicising their personal contact details on any social media platform or website, to avoid unwanted contact by parents/carers or students.

Staff must not use their personal mobile phones to take photographs or recordings of students, their work, or anything else that could identify a student. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

3.4 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but are not limited to:

- Use of multi-factor authentication
- Emergency evacuations

3.5 Work phones

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct and acceptable use policy.

4. Use of mobile phones by students

Key Stage 4 Students

In line with the instructions given by the Minister for Education and Lifelong learning in June 2025, Government of Jersey Schools and Colleges including Hautlieu will not allow phone use at any time during the school day (which begins as soon as a student enters the building and ends once a student has left the building), including break and lunch times for all students up to the end of Key Stage 4. If a student brings a mobile phone into school, then it must be switched off, not visible and kept in their bags at all times. Frequent reminders will be given through assemblies and Mentor time messages.

Medical exemption

Key Stage 4 students who have a medical exemption (e.g mobile phone is used for medical updates linked to insulin pumps) may keep their mobile phone switched on in their bags. Students who

have permission will be issued with a sticker with the letter 'M' which will be stuck to the back of their lanyard card holder. In addition, their names will be circulated to all staff and the exemption added to a quick note in SIMS by the EWO responsible for Health Care Plans.

Key Stage 5 Students

For Key Stage 5 students, during lessons mobile phones are not to be seen or heard unless prior permission has been sought by the student from their teacher. Such circumstances may include but are not limited to:

- Using a mobile phone to take photos of the board to support with note taking
- Using a mobile phone for learning purposes such as but not limited to Satchel:One, Seneca, DrFrost Maths, OneNote. This is always through direction from a member of staff

Key Stage 5 students are able to use their mobiles phones during non-contact time around the school building during the school day in a responsible and safe manner.

For more detailed guidance, please refer to Student ICT Acceptable Use Policy (Appendix 2)

4.1 Sanctions

Key Stage 4

If a mobile phone is found in use during the school day, the phone will be taken from the student and be stored in the school office, placed in an envelope with the student's name on it. The phone can be collected at the end of the day.

When a staff member has taken a mobile phone from the student, they are responsible for placing it in an envelope with the student's name on the front and delivering it to reception. They must also log under SIMS|Behaviour|Mobile Phone as soon as possible.

If a student refuses to hand over their mobile phone, then Senior Leadership will be contacted for support. Should a student have their mobile phone taken from them on more than one occasion, then parents will be contacted and asked to collect the phone from Main Reception.

Key Stage 5

Any phone usage must adhere to our Behaviour for Learning Policy and Acceptable Use Agreement and a serious breach of this will result in the phone being taken from the student.

When a staff member has taken a mobile phone from the student, they are responsible for placing it in an envelope with the student's name on the front and delivering it to reception. They must also log under SIMS|Behaviour|Mobile Phone as soon as possible.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. Hautlieu takes such conduct extremely seriously and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault

- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

5. Use of mobile phones by parents/carers, volunteers and visitors

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to 'The Guidance for Visitors to Hautlieu'

This means:

- There is no use of photographic, video or audio equipment on site without prior agreement of a Deputy Headteacher or Headteacher
- The use of IT equipment, access to network etc. must comply with acceptable use policy (Appendix 1)
- If you would like to share on a social media about a visit to Hautlieu, then the Business Manager needs to be contacted.

6. Loss, theft or damage

In line with the instructions given by the Minister for Education and Lifelong learning in June 2025, if a Key Stage 4 student brings a mobile phone into school, then it must be switched off, not visible and kept in their bags at all times.

Key Stage 5 students must secure their mobile phones as much as possible, including using passwords or pin codes to protect access to the phone's functions.

Staff must also secure their personal phones, as well as any work phone provided to them. Failure to do so could result in data breaches.

Hautlieu School accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while Students are travelling to and from school.

When a phone is taken from a student it will be stored in the school office, placed in an envelope with the student's name on it. The phone can be collected at the end of the day.

Lost phones should be handed in to the school office. The school will then attempt to contact the owner.

7. Monitoring and review

Hautlieu school is committed to ensuring that this policy has a positive impact on Students' education, behaviour and welfare in accordance with the instructions from the Minister for Education and Lifelong Learning in June 2025.

8. Links to UNCRC – Rights Respecting Schools

This policy links to the following UNCRC articles:

Article 1: Everyone under 18 has all of these rights

Article 2: You have the right to protection against discrimination. This means that nobody can treat you badly because of your colour, sex or religion. If you speak another language, have a disability or are rich or poor

Article 3: All adults should always do what is best for you

Article 12: You have the right to express views on matters affecting you

Article 28: You have the right to an education

Article 29: Education must develop talents and abilities to the full

Article 42: All adults and children should know about this convention. You have the right to learn about your rights and adults should learn about them too.

9. Useful Links

- Jersey Keeping Children Safe in Education
- Guidance for visitors to Hautlieu

10. Links to other policies

This policy is linked to:

- Behaviour for Learning Policy
- Counter Bullying Policy
- Acceptable Use Policy – Students and Staff
- AI Policy

Review dates:

Date	Updates	Person responsible
24.6.26	- Minor revision to clarify what 'school day' means. - Update of Staff and Student AUP	CMJ RSM

11. Appendices

Appendix 1: CYPES Acceptable Use Policy

Acceptable Usage Agreement for Staff in Educational, Youth Service and Residential Care Settings

Document Purpose	To outline the appropriate use of IT equipment and platforms.
Author	CYPES Governance Team (Digital)
Publication Date	13/11/2024
Target Audience	Staff working in Education, Youth Service and Residential Care settings All other GoJ staff should refer to the Central Acceptable Use Policy
Circulation List	All CYPES staff in Education, Youth Service and Residential Childcare Settings
Description	This Acceptable Usage Agreement outlines the responsibilities and acceptable behaviour expected of all staff when using any technology for work purposes, and when - communicating with students, parents, colleagues, and other stakeholders.
Linked Policies	1. Remote - Home Working Policy (Info-Sec-Pol- 013) - Information security policies 2. BYOD (Bring Your Own Device) Policy (Info-Sec-Pol-012) - Information security policies 3. CYPES Clear Desk re& Screen Policy 4. Information Classification Policy (Info-Sec-Pol- 005) - Information security policies 5. RM-POL-001 – Corporate Records Management Policy - Records - Home (sharepoint.com) 6. Data Protection Policy (or contact dataprotection2018@gov.je) 7. Retention Schedules - Children, Young People, Education and Skills retention schedules (gov.je) 8. Individual School Policies 9. CYPES Data Security policy

	10. AI Policy - P AI In Jersey Education Policy 20231006.pdf (gov.je) 11. Online Safety policy 12. CYPES Wi-Fi/Unknown network guidelines 13. CEYS – Early Years Statutory Guidance
Approval Route	Education SLT CSC SLT COD DLT
Review Date	November 2025
Contact Details	cypesgovernance@gov.je cypesdigital@gov.je

Overview

This Acceptable Usage Agreement outlines the responsibilities and acceptable behaviour expected of all staff working in Education, Youth Service or Residential Care Home settings when using any technology for work purposes and when - communicating with students/children, parents/guardians, colleagues, and other stakeholders.

1. Scope

This agreement applies to:

- *All staff, including permanent, temporary, visiting employees, contractors and other 3rd parties with access to school, youth service, residential care home, government systems and technology.*
- *The use of all digital technology, Internet and electronic communication platforms (e.g., emails, learning platforms, Wi-Fi, school systems).*
- *Personal and professional usage of devices within educational, youth, residential care homes and other GoJ sites.*

Monitoring

All systems are continuously monitored and periodically audited. The purpose of this activity is to ensure that threats to systems and data are identified as early as possible to minimise impact to the business and to ensure the safeguarding of the children in our care.

If illegal activities are detected, GoJ will inform law enforcement and regulatory agencies such as Jersey Office of the Information Commissioner (JOIC) as required.

1.1. Monitoring of user activity

- *Tools to support safeguarding are used in all Educational, Youth Service and Residential Care Home sites, these are used to filter internet use and monitor device and internet use.*
- *GoJ detects unauthorised activity by recording what information has been accessed, by whom, and when it was attempted. GoJ needs to determine if this activity is suspicious and where necessary, prevent any further misuse or harmful effects. If the activity is violating policy requirements, action will be taken as described in Section 3 above.*

- *GoJ also has legislative requirements to be open and transparent. GoJ will seek appropriate authorisation before performing data discovery processes. These are a combination of automated and manual collection processes to satisfy the authorisation. Discovery processes will examine (but not limited to)*
 - *data storage platforms (e.g., files on your computer, shared devices and Government, Education, Youth Service and Residential Care Home IT systems)*
 - *collaboration platforms (e.g., Intranet sites, ticketing systems)*
 - *communication platforms (e.g., emails, chat and meeting history and other messaging systems).*

1.3. Incident Reporting

- *If an incident occurs within a school setting*
 - *you must immediately notify the schools Data Protection Officer and follow the school guidance.*
 - *Alternatively, you may refer to your line manager.*
 - *If immediate action can be taken i.e. recovering a lost document or device, then please undertake this and document any actions.*
 - *you must report any security concerns as soon as you become aware of them. You can do this by raising a security incident via the button on the MyStates home page (<https://soj>)*
- *If you are outside a school setting eg a Youth site or Residential Home or are a schools Data Protection Officer*
 - *you must report any security concerns as soon as you become aware of them. You can do this by raising a security incident via the button on the MyStates home page (<https://soj>)*
 - *you should engage with your Departmental Governance representative to support you (cypesgovernance@gov.je). This requirement extends from potential weaknesses to actual breaches and policy violations. CYPES will work with Departments to log and track the issue and correlate it with any similar events that occur. – For further details, please refer to the CYPES Data Security Policy.*
 - *If immediate action can be taken i.e. recovering a lost document or device, then please undertake this and document any actions.*

1.a.3. Email archival

- *All @gov.je and @health.gov.je emails sent and received, internally and externally, are automatically archived in a secure forensic archival system. Users should therefore be aware that all messages, even if deleted or altered in Outlook, will be retrievable for a period determined by data retention schedules and may be used to satisfy legal requirements for example Subject Access Requests (SARS) and Freedom of Information (FOI) requests. This does not supersede any Departmental email management processes.*
- *For all staff once emails are deleted, be aware they remain in your deleted folder. One removed from your deleted folder they then move to the super deleted folder where they are still recoverable. Once removed from this folder they are non-recoverable.*

3.3. Personal use and privacy

- *GoJ permit limited personal use of GoJ provided internet and email systems, providing that it follows this policy and does not adversely affect your work. However, you are discouraged from storing your personal data on GoJ systems.*
- *Where this is unavoidable this activity is done entirely at your own risk, and GoJ cannot be held liable for any claims arising from the unauthorised disclosure or loss of your personal data held by you in this way.*

- *Here personal data means data belonging to an individual and not the meaning under the Data Protection (Jersey) Law 2018 which is "any data relating to a data subject". The Government is not processing this data, has not recorded this information for processing or recorded it as part of a filing system.*
- *As this information is stored on GoJ systems, it will be discoverable and may be disclosed as part of eDiscovery*
- *If you logged in to M365 services on a personal device, this may be monitored.*

Acceptable use of Technology

4.1. Looking after School/GoJ/Youth/Residential Home-Owned equipment

The term 'equipment' includes (but is not limited to) computers, smartphones, and tablets issued to you by GoJ or by any GoJ managed School, Youth site or Residential Care Home. The equipment assigned to you must:

- be used for the purposes for which it was intended
- be protected from damage, unauthorised access and theft
- be reported immediately to the School or Central EDU IT Service Desk if lost or stolen and be reported as a Security Incident via MyStates.
- at the end of contract, any equipment must be returned to the relevant site.
- Be aware of any additional policies relating to school purchased equipment.

4.2. Preventing unauthorised access

Regardless of your role, the facilities that you work in hold information and systems that must be protected from unauthorised access. You must:

- lock your computer/tablet/smartphone when left unattended for any period of time.
- clear paperwork away if leaving your work area for any significant length of time (e.g. meetings or breaks). Please refer to the Clear Desk Policy for further details.
- return paperwork into relevant filing systems at the end of the working day.
- close windows in your vicinity.
- do not let anyone borrow your ID to gain access to restricted areas.
- challenge individuals you do not recognise and who are not wearing an ID.
- You are prohibited from plugging in any networked or storage equipment not provided to you (e.g. mobile phones, USB storage device) into school/GoJ-owned equipment.

4.3. Passwords and passphrases

Passwords are used in combination with your user ID to grant access to various services. They can also be used to protect OFFICIAL-SENSITIVE (and above) data when being shared or stored.

Instead of using passwords, it is recommended for you to use a passphrase - a combination of several words together. This is easier for you to remember and more difficult to guess.

To build strong passphrases, you must:

- use a minimum of 15 characters
- combine unrelated words together.
- use symbols to separate words (e.g. full stop '.', hyphen '-')
- add additional numbers and symbols if it makes it more memorable You must not use passphrases that:

- use a single dictionary word, in any language
 - are examples used on the internet or in training materials (e.g. correct-horse-battery-staple)
 - use simple keyboard patterns (e.g. qwertyuiop12345)
 - use symbols that look like letters (e.g. P@ssW0rd)
 - On rare occasions that you need to share a passphrase (e.g. when sharing a password protected document and need to share the password)
 - do not send the attachment/passphrase using the same technology (e.g. email)
 - send them via different methods (e.g. send by email, provide password over the phone)
 - be discrete if you are sharing passphrases via phone calls
 - delete passphrases stored electronically when no longer needed.
 - If you suspect that your user account or passphrase has been compromised, change your passphrase immediately and log it via "Report a Security Incident."
- 1.4. Multi Factor Authentication (MFA) MFA MUST be enabled and utilised.
- 1.5. Working remotely

The need to working remotely is an identified requirement. In order to support this you may be provided with:

- portable equipment
- secure access to services from a personal device, such as access to M365.

1.5.1. Working remotely with your equipment

You may be provided with equipment that is portable and usable outside of your working location. When using this portable equipment in public, ensure that you are in complying with the [Remote-Home Working Policy](#)

For guidance on connecting to public Wi-Fi, please see CYPES Wi-Fi/Unknown network guidelines.

4.5.2. Working remotely to access specific services

When working remotely on personal devices, you must access all information via the services provided and interact via these services. You must not download a copy of this information and store it locally.

4.6. Control failure does not imply permission

The failure of security tools and controls to block certain actions should not be taken as implied permission to ignore policy requirements. You must immediately report any failures as a Security Incident via MyStates.

5. Acceptable use of communications

5.1. Use of the internet

GoJ provides access to the internet for business and education purposes. Since Government cannot guarantee the security of internet resources, you must NOT:

- download, run or install software from the internet, without permission.
- use any internet hosted storage services that are not approved (e.g. OneDrive for Work/School and Egress)

- intentionally access, download, store, process, publish, display or send media (e.g. videos, photos and audio) that are illegal, pornographic, discriminatory, hateful or likely to offend
- reproduce news articles, blogs or other external media, as they may be subject to copyright law. Obtain permission before using or circulating such media from the blog writer or media organisation
- intentionally try to access Government information or systems that you are not authorised to access

5.2. Use of email

Suspicious emails (e.g. virus warnings, security threats, offers, scams, chain emails) should not be opened, replied to or sent onto colleagues. For further guidance, search for "Phishing" on the Intranet.

Other email good practices to follow are:

- avoid sending files wherever possible; instead send a link to the file location (e.g. on SharePoint or Teams)
- avoid embedding attachments in Calendar invites, instead provide a link to the file location (e.g. on Teams or Shared drives)
- where you need to send data classified under the Information Classification Policy (Info-Sec-Pol-005) as OFFICIAL-SENSITIVE or sensitive personal data this needs to be encrypted and sent using the approved secure email solution (i.e. Egress). Please contact the Governance Team for support and guidance.
- using the "Bcc:" field rather than "Cc" when sending emails to third parties, and when communicating with many recipients
- avoid broadcasting emails to lots of people. Instead, limit the recipients to those who need to know
- convert documents to PDF when being sent externally. PDFs preserve the integrity of their contents and minimise the risks associated with sending hidden data by mistake.

You must NOT:

- sign up to websites or services with your work email address, unless required to as part of your role (e.g. procurement, training, equipment purchasing, service notifications)
- use it as a primary point of contact for your personal affairs (e.g. banking, healthcare, legal advice)

1.1. Use of voice and post

When speaking about sensitive matters, be aware of the risks of being overheard. To maintain the confidentiality of sensitive information:

- use meeting rooms or close the door of the room you are in
 - use headphones when making calls from your phone or computer and ensure you are discreet when relaying sensitive information (e.g. Teams calls)
- If posting or sending sensitive information by courier, ensure the package is appropriately labelled so as not to describe its contents.

1.2. Unacceptable Use

For the avoidance of doubt, the following behaviours are considered an unacceptable use of Government systems, therefore are direct violations of this policy:

- intentionally disabling or bypassing security controls

- making unauthorised copies of information, passing information to third parties without authorisation, or retaining information after your contract of employment has ended.

6. Acceptable use of information

6.1. Information classification

All information, whether electronic or paper-based, must be protected according to its sensitivity and the impact of a breach. The key principles are:

- there are three broad classification levels: OFFICIAL, SECRET and TOP-SECRET
- most of the day-to-day business of government, service delivery, commercial activity and policy development is classed as OFFICIAL
- if you need to emphasise that the artefact is for a restricted audience, add the sub-category SENSITIVE to imply these constraints are necessary, i.e. OFFICIAL-SENSITIVE eg for Safeguarding
- Where such classification has not been applied, it should be deemed OFFICIAL by default
- additional protective controls may be required. Please refer to the Information Classification Policy (Info- Sec-Pol-005) for more information.

For further guidance, please email cypesgovernance@gov.je

1.1. Information handling

Your employer is the owner of all information you produce during the normal course of your employment. Therefore, you must protect the integrity of this information during its use.

When handling information, you must:

- Be aware each school is a separate Data Controller
- apply an appropriate classification label as described in [Information Classification Policy \(Info-Sec-Pol- 005\)](#)
- store the information securely with appropriate access controls for that classification level
- send a link to the information if it is stored internally, or a PDF copy if sent externally. The original version should be considered when first two options are unsuitable
- gain formal authorisation / data sharing agreements for sharing large quantities of data across departments, with external suppliers or other schools. Contact your Department Governance representative for support and guidance (cypesgovernance@gov.je). When considering sharing data across departments, with external suppliers or with other schools, refer to the Privacy Policy of the Data Controller.
- Data sharing must only be done with a specific purpose and lawful basis
- When the decision has been made to destroy information (please refer to your retention schedules), use confidential shredding bins or deletion.
- If using AI, data must be handled in line with the [AI Policy](#).

1.2. Document Management

Documents created as part of your day-to-day work must be stored on:

- your department/schools document management system e.g. SharePoint
- an agreed Microsoft Teams or SharePoint site
- printed to paper (where this is required, though Government preference is to operate in a paper-lite manner) and placed in the appropriate filing system.

1.3. Retention Schedule

- All data is subject to being destroyed in accordance with the relevant data retention schedule. These can be found here: [Children, Young People, Education and Skills retention schedules \(gov.je\)](#)

7. Agreement Name :

Signature:

Date

:

Hautlieu School - Acceptable Use Policy (Students)

You must not use any ICT in Hautlieu School until you and your parents have signed this document. Please read it carefully and ensure that you have fully understood the document before signing.

- 1.** I agree that the rules contained in this document will apply to me at all times when I am using ICT hardware (computers, mobile phones, peripherals, etc.) and facilities (software, networks, charging sockets, etc.) in Hautlieu School even if the equipment that I am using belongs to me.
- 2.** I will only log into the Hautlieu school network using my Hautlieu account and not any other accounts I may have used in previous schools.
- 3.** I will not deliberately modify, damage or vandalise school ICT equipment. If I accidentally break anything then I will tell a teacher straight away.
- 4.** In bringing my own ICT equipment to school then I will obey all the extra rules I will be given about how I can use my ICT equipment on-site. I agree that all traffic to and from the internet will be de-encrypted as part of the proxy service run by the department for Children, Young People, Education and Skills. I understand that the school will also monitor the content of the searches that I make and websites that I visit on a daily basis. I also agree that my ICT devices can be inspected at any time by teachers and may be confiscated if a teacher decides this is necessary.
- 5.** I realise that my use of home-owned equipment in school and school owned ICT devices will be monitored and that **everything** I do may be recorded. I agree that I have no right to privacy and I agree to being monitored and recorded at all times. I realise that the results of this monitoring may be shared with other people if I break any of the rules or if my actions are of a criminal nature.
- 6.** I will not access any websites, services (including proxy), files or other resources that are blocked or which I know that I am not allowed to access.
- 7.** I will always log-in to the school network using my own user name and password: I will not disclose my log-in details to anybody else. I agree that I will be responsible for everything that is done using my log-in details and for all files that are held in my personal storage area, and lock my workstation when I need to leave it unattended for a short period of time. If I think that somebody else has discovered my log-in details then I will tell a teacher / ICT Technician immediately so that my log-in details can be changed.
- 8.** I agree that my use of ICT devices belonging to Hautlieu School will mainly be for educational purposes unless I have permission from a teacher for other uses at specific times. I understand that I can carry and use personal devices, but when in Year 10 & Year 11 I am not permitted to use a mobile phone during the school day whilst on site (Year 12 & Year 13 may use mobile phones during the school day whilst on site)
- 9.** I will only print documents relevant for school use and will not print inappropriate documents or images. I will intentionally check the location (printer) to which I send print jobs to avoid wasting school resources.

10. I agree never to illegally download or upload copyright materials. Downloading copyright materials (including music and video files) without paying the appropriate licence fee is often a criminal act that will be treated as theft.

11. Proper conduct must be maintained at all times while using ICT. I agree that I will not harass, bully, insult or attack others via email, social media or any other means. The use of strong language, swearing or aggressive behavior is not acceptable. I will be polite at all times and report any concerns I have to a teacher or my mentor. I understand that the school will help me in dealing with any incidents I am a victim of, or take disciplinary action where my conduct is unacceptable and harmful.

12. I agree that I will not try to view, send, upload or download material that is unsuitable for viewing in Hautlieu School including any youth produced sexual images which are illegal to produce, share and be in possession of. If I accidentally see any unsuitable material then I will immediately close (but not delete, in the case of emails and social media) the material and tell a teacher. I know I will not be punished if I view unsuitable material by accident and I realise that by reporting this I will help to improve e-safety within Hautlieu School.

13. I will carefully consider how I disclose my personal details such as my home address and personal telephone numbers when online. I realise the importance of scrutinizing privacy policies on websites and apps in order to protect my personal data. If I disclose any data on the school network then I agree that Hautlieu School will not be responsible for maintaining the security of the details that I have given. I agree that I will never pass-on the personal details of another person without that person's permission.

We would be grateful if you would carefully consider both the advantages and disadvantages of having access to the School Network and Internet, reflect on the acceptable ways in which any form of device should be used in school and then complete the authorisation below.

Hautlieu School - Acceptable Use Policy (Students)	
Student: As a school user of the computers and Internet, I agree to comply with the school rules on its use, as described above. I understand that if I break any of these rules then my access to ICT in Hautlieu School may be restricted or ceased. I understand that any inappropriate activities may also be reported to external authorities such as the police.	
Student Name	
Student Signature	
Date	

Parent/Carer	
As the parent or legal guardian of the student signing above, I grant permission for my child to use computers, electronic mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.	
Parent Responsible	
Parent Signature	
Date	

Additional e-safety information for Students.

You have signed the Hautlieu School Acceptable Use Policy (AUP) for ICT equipment/facilities and you have agreed to obey the rules that the AUP contains. Copies of the AUP can be gained on request from the main or ICT office.

As well as the rules that you have agreed to obey there are also some extra guidelines that will help to keep you e-safe.

- a)** Be very careful when replying to emails or messages from unknown senders.
- b)** Be very careful if you agree to meet somebody whom you have previously only known online: remember that online identities are very easy to fake and the person who you are planning to meet may not be who he/she claims to be. Always tell somebody where and when you have arranged a meeting and take a responsible friend with you.
- c)** Do not make hurtful comments about another person: cyber-bullying and online bullying will not be tolerated by schools. If you think that you have been the victim of any form of bullying please report it to a member of staff as soon as possible. Be mindful at all times that information shared digitally can be misconstrued so you need to be careful about what you say to others.
- d)** Remember that everything you do in cyberspace leaves a “digital footprint”. If you post a silly or potentially embarrassing photograph of yourself, or somebody else online then that image may be copied, changed and distributed without your control and for a long time into the future. It is frequently impossible to completely remove any material that has been uploaded to the Internet.
- e)** Be very careful about discussing any aspect of the Hautlieu School community on other websites as this may lead to accusations of inappropriate behaviour that could result in you being punished under the terms of this Acceptable Use Policy.
- f)** In the context of this Acceptable Use Policy, “unsuitable” material is any material that a teacher says is “unsuitable”. If you are not sure about whether a specific item (document, image, audio file, video clip, etc.) is “unsuitable” or if another person has any doubts about whether material is “unsuitable” then you must not continue to access the material until you have been given permission to do so by a teacher.

ICT Acceptable Use Policy - Hautlieu School

Hautlieu School currently houses an extensive network of computers and has a school wide Wi-Fi provision that staff, visitors and students can access on personal devices such as laptops, mobile phones, iPads etc.

With this in mind students are encouraged to use the facilities to their full potential which in turn provides a great benefit to their day to day learning.

Before a student can gain access to the ICT resources they must first sign an acceptable use policy. Students are required to state their intention to use the infrastructure appropriately and in accordance with the acceptable use policy. Secondly, students must agree to allow the school to monitor student usage across the network on any device, be it with the use of monitoring software or simply checking through their files / home folder.

With these guidelines in place it allows Hautlieu to continue to offer exemplary ICT resources to students.

Before being allowed to use the Network, all students must obtain parental permission and both you and your child must sign below as evidence of your approval and their acceptance of the school rules on this matter.

Please be aware that failure to comply with the acceptable use policy could result in disciplinary action.

Internet & E-mail Access

With the use of our high speed Internet connection, ease of access to the global network of computers and the capabilities of 3G, 4G and 5G networks, educational resources such as libraries, databases and bulletin boards along with the use of E-mail are all openly available as are non-educational resources such as social media. Families should be warned that some material accessible via the internet, including via mobile devices, contains items that are illegal, defamatory, inaccurate or potentially offensive to students, their peers and others.

Hautlieu has a highly effective Internet filtering system for both the wired and wireless network. Rarely can students access undesirable content either maliciously or without intent whilst using the school network. We will endeavor to restrict access to this type of content through filtering. Unfortunately, it is sometimes hard to find a happy medium between open and restricted access and over restriction may cause the global and dynamic nature of the internet to be lost. Additionally, with the worldwide capabilities of 3G, 4G and 5G we are aware that students can also access material through their mobile devices, which is outside of the school's control whilst onsite and under school supervision.