CLAYESMORE

# ICT AND INTERNET ACCEPTABLE USE AGREEMENT & POLICY FOR SENIOR SCHOOL STUDENTS, ALL STAFF & GOVERNORS

| | |
|---|---|
| Responsible: | Head of Compliance |
| Date Reviewed: | 16 January 2025 |
| Review Period: | Annual |
| Scope: | Senior School |
| Approval Authority: | SLT |
| Approval Date: | 06 February 2025 |
| External Release: | Yes |

CONTENTS

## INTRODUCTION

Advancing technologies have become integral to all our lives, whether we be staff using technology to perform our roles, or students using Information and Communication Technology (ICT) to further our education. The School will seek to ensure that all ICT users have access to excellent ICT and safe internet facilities and in return we expect all users to be responsible.
The key to safe internet use is training and open discussion. Clayesmore assumes everyone will read this document and that parents and guardians will read and discuss this agreement with their sons and daughters. This agreement is intended to ensure:

- Young people will be responsible users and stay safe while using the internet and other ICT for educational, personal and recreational use.
- Staff use ICT systems in a manner that is responsible and appropriate.
- The School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

### Purpose

The purpose of this document is to outline the School's policy on the acceptable use of the ICT facilities provided by Clayesmore, including acceptable access to and use of the internet.
It outlines what is considered to be acceptable use and what is not and provides information about sanctions for non-compliance and/or malicious activity.

The School recognises an individual's rights to privacy but needs to balance this with the requirement to act appropriately and reasonably to ensure the safeguarding of the children in our care. Therefore, in applying this policy, we will act in accordance with current legislation and statutory instruments, including the Human Rights Act 1998, and will recognise the need for individuals to maintain an appropriate work/life balance, whilst protecting their welfare and wellbeing.

### Scope

Clayesmore ICT facilities are provided for the purpose of Clayesmore School business and this acceptable use policy applies to:

- All users of the services provided by Clayesmore including students, staff, visitors, staff partners/spouses/families, third parties, contractors and associates. Access to School systems is not intended to confer any status of employment on any contractors.
- Any equipment/devices owned by Clayesmore, or equipment/devices that Clayesmore has facilitated access to, including all forms of communication and information retrieval.
- The use of privately owned ICT devices of all kinds whilst accessing the internet through Clayesmore ICT facilities (cable or WiFi) including web browsing, email, social networks, chat rooms, blogs, gaming, media streaming and learning environments.

In order that all members of the School and its employees understand this policy and the rules placed upon them the agreement will be signed when people join the School, or whenever the policy is significantly revised and reissued.

This includes:

- Students in Year 9 and above (years 8 and below adhere to the policy HERE)
- Parents or guardians
- Staff, governors and volunteers
- Any other individual (including staff partners/ spouses/ family/ visitors/ contractors) who have access to the School's ICT facilities.

## POLICY REQUIREMENTS AND CONSEQUENCES

### Cyber Bullying

Cyber-bullying is an aggressive intentional act carried out by an individual or a group using electronic media against victims who cannot defend themselves. Any of the following can be used inappropriately in cyber-bullying: text messaging including pictures and videos, mobile phone calls, e-mail or other messaging, defamatory blogs or websites and inappropriate use of social network sites such as Facebook or Snapchat.

These forms of bullying have a direct impact on the health and happiness of the victim.
In the event that such bullying emanates from an individual or group within Clayesmore, the perpetrators will be subject to disciplinary action.
Anyone who is the victim of any form of cyber-bullying or feels uncomfortable about anything should talk to their parents, tutor, Housemaster/ Housemistress, a Deputy Head, Department Head or any other member of staff as appropriate.

### IT Etiquette

The School cannot guarantee the confidentiality of content created, shared and exchanged via School systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by. The GDPR and DP laws require us to pass on any emails that exist within our systems to the subject of a Subject Access Request, no matter how embarrassing.

Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
Do not access or share material that infringes copyright, and do not claim the work of others as your own.

Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
Honour the rights of others by not using the School network for extended periods of time or for lengthy tasks that should be carefully scheduled.
Only print out material that is required for course work or further research.
Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

### Using the School's IT Systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Pay careful attention to the appropriate training provided to use internet services efficiently and effectively.
- During the School day and during study hours, only use the internet services with an academic goal or purpose. This does not exclude exploration activities with a learning objective, but does exclude any or all activities that cannot be academically justified.

- Games may be played after formal commitments end for the day. They may not be accessed between 8.15am and 5.15pm nor after lights out.
- Large downloads must not be made during the working day. Films may be watched after school commitments end for the day but not during prep or after lights out.
- Only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not use your clayesmore.com email address for personal matters.
- Do not attempt to install software on, or otherwise alter, School IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and through a system called Netsweeper, the School can view content accessed or sent via its systems.
- Accessing, uploading, downloading, transmitting or displaying or distributing obscene or sexually explicit material transmitting obscene, abusive or sexually explicit language is strictly prohibited and against the law.

**Using School Property**

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the ICT Department.

**Data Security, Passwords and 2FA**

Schools hold personal data on students, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisations to cause harm or distress to an individual. The loss of sensitive information can result in media coverage and potentially damage the reputation of the School. Therefore, everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be aware of the risks and threats and how to minimise them.

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthday), and nor should they be the same as your widely-used personal passwords.
You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

The use of Two Factor Authentication (2FA) is now mandatory on all Clayesmore staff accounts. It is also strongly recommended that all staff use 2FA for their personal accounts as it is a significant protection against hackers and identity theft.
The use of memory sticks by staff is forbidden without specific permission as the potential risk of a data breach is significant with these devices. Staff have access to, and should use as a first option, Google Drive and associated software for the sharing and remote access of documents.

**Monitoring of Accounts**

The provision of School email accounts, Wi-Fi and internet access is for official School business, administration and education. Staff and students should keep their personal, family and social lives separate from their School IT use and limit, as far as possible, any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

Staff, parents and students should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding, conduct and performance purposes and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose, including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by students, whether or not such devices are permitted, may be confiscated and examined under such circumstances.

The School may require staff to undergo searches of their personal accounts or devices if they were used for School business in contravention of this policy and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

**Education and Training**

The School understands its responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is explained to staff during induction and an electronic link provided for future reference. Clarification on any points should in the first instance be sought from a senior member of staff, Head of IT Support & Systems or the Head of Compliance. This policy complements, and should be read in conjunction with, the Staff Code of Conduct.

**Staff Mobile Phones, Personal Devices/Accounts and Working Remotely**

All official School business of staff and governors must be conducted on School systems, and it is not permissible to use personal email accounts for School business.

Any use of personal devices for School purposes, and any removal of personal data or confidential information from School systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Head, Director of Finance & Operations or the Head of Compliance.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including two-factor authentication, encryption etc.

**Student Use of Mobile Phones and Other Devices**

- Please refer to the Student Use of Mobile Phones policy, that can be found HERE.

**Data Protection and Reporting of Data Breaches**

- All staff, parents and students need to be aware of the direction, guidance and requirements of the School's Data Protection Policy, which should be read in conjunction with this policy.

**Emergencies and Exceptions**

If a student needs to contact his/her parents/guardians they may phone from the Main House Reception, the house office or Mrs Lockwood's office. In exceptional situations, they will be allowed to use their mobile phone to contact parents, but only with explicit permission from a member of staff.

If parents need to contact their child during the working day, they may email or phone the house matron, School Reception, Mrs Lockwood's office or the student's tutor and a message will be given to them as soon as possible.

**Consequences and Sanctions**

Infringements of this policy will be dealt with under Clayesmore's disciplinary procedures for staff and students as appropriate and potential sanctions may include:

- Withdrawal of access to Clayesmore ICT facilities.
- Seizure of equipment/devices used in violation of this policy.
- Detention, suspension or exclusion of students from Clayesmore.
- Disciplinary action or termination of contract for staff.
- Where criminal offences are suspected or detected the matter will be referred to external law enforcement and/or child protection agencies for advice, guidance or investigation.