ICT Acceptable Use Policy

Diversity, Equality & Inclusivity Statement:

The commitment to diversity, equality, and inclusivity is at the heart of our values at Austin Friars. Equality means creating an environment where pupils have the chance to achieve their full potential, free from barriers, prejudice, and discrimination. Inclusion is about recognising that each pupil is unique and that their needs can be met in different ways. Diversity means recognising, respecting, and celebrating the added value that differences bring. Our unwavering dedication to our school values – Truth, Love and Unity - is how we fulfil our mission at Austin Friars. It is through our commitment to diversity, equality, and inclusivity that our pupils are empowered to be authentic and succeed.

This policy is the responsibility of the Deputy Head (Academic) and will be reviewed biennially.

Scope of the Policy

This policy applies to all members of the School community, including staff, pupils, and visitors. In this policy 'staff' includes teaching and non-teaching staff, Trustees, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Visitors' includes anyone else who comes to the School, including parents, carers and occasional volunteers. Access applies to the School's Wi-fi network and the use of 3G and 4G on personal devices whilst on the school site. This policy does not form part of any contract and it may be amended at any time.

Online Behaviour

The ICT system at Austin Friars is provided as a work tool to enhance teaching and learning. Access to the School's system is provided on condition that the guidelines and good practice set out in this policy are followed. It equally applies to members of the School community who wish to use their own laptop, smart watch or other mobile device during the School day. **As a member of the School community you should follow these principles in all of your online activities.**

(a) 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. Electronic media should not be used to harass or insult others and this is deemed to be bullying. Any email sent can be traced and the recipient of an offensive email may take legal action against the sender.

(b) 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 offensive, promotes violence, discrimination or extremism or raises safeguarding issues). Any material which the School considers inappropriate or offensive, will be removed immediately.

(c) 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. Use of personal information, contrary to the provisions of the Data Protection Act 2018 is a serious offence.

(d) Do not access or share materials that infringe copyright and do not claim the work of others as your own. All resources in written work and non-examination assessments must be acknowledged, including where AI is used. Examination Boards utilise software to check for plagiarism, including in previously submitted work. The unauthorised copying of software and media is contrary to copyright law.

(e) 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.

(f) All official School business must be conducted on School systems **unless there is no practical alternative**. It is not permissible to use personal email accounts for School business in any situation. Staff should not use their personal email or social media accounts to contact pupils or parents on school business.

(g) When delivering lessons via *Zoom*, or *Teams*, staff should adhere to the guidance set out in the Online Teaching and Learning Policy. Pupils and parents should not attempt to identify the personal email addresses or social media accounts of staff.

(h) Staff must act in accordance with the guidance given in the School's Online Teaching and Learning Policy (Appendix 2)

(i) Users may only attempt to install software on a School computer or run it from a peripheral memory device if this has been authorised by the ICT Systems Manager.

(j) Although the School IT system is backed up on a regular basis, it is the responsibility of staff who have portable devices, which can connect to the School system, to back up their files on a regular basis.

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:

(a) Users are responsible for the use of their account on the School network and for compliance with the School's Social Media policy. All access to the internet including sites visited by each user is logged. **Only access School IT systems using your own username and password. Do not share your username or password with anyone else.** Computers should only be left unattended after the logging off procedure has been completed. 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 "birthdays"), nor should they be the same as your widely used passwords. You should not keep a list of passwords where they may be accessed and must change your password 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.

(b) The Internet and email system is filtered to stop inappropriate sites from being accessed. If, however, a web page which is offensive is accessed accidentally, it should be immediately reported to the ICT Systems Manager who will take the necessary action to prevent further access to the site.

(c) Do not attempt to by-pass any 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.

(d) Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.

(e) Staff, parents and pupils should be aware that School email and internet usage is 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 misconduct, welfare concerns, extremism and the protection of others.

(f) Any property belonging to the School should be treated with respect and care and used only in accordance with training and policies provided. You must report any faults or breakages without delay to the ICT Systems Manager and ensure computers and their surrounding areas are left clear and in good working order for the next user.

Use of 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 Systems Manager. Intentional damage to computers, computer systems or computer networks, including unauthorised damage, interference or unauthorised access to any files may be considered a criminal offence.

On those occasions when a member of staff requires the use of School equipment at home; other members of the household must not be able to access data either stored on these devices, or on the school network, and so staff must either lock, or sign out of the device when not in use.

School IT devices should not be used for personal use or private business; any data stored on school devices is under the ownership of Austin Friars.

The Internet and email

a) The provision of email accounts, Wi-Fi and Internet access by the School is for official School business, administration and education. Access is a privilege, not a right, and that access requires staff and pupils to be responsible at all times for its proper use. Staff and pupils 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.
b) Users should be aware that every website visited is logged. Email messages may not be sent or received during lessons or prep without the permission of a member of staff.
c) Unauthorised entry into chat rooms is forbidden.
d) Unidentified email attachments should not be opened and pupils should not complete questionnaires or subscription forms online without the permission of a member of staff.
e) Staff and pupils must be aware that all emails sent or received on School systems will not be routinely deleted. Staff are asked to ensure that they regularly delete unwanted (not required for a purpose) emails in line with the School's retention policy.

f) Email accounts will be closed within half a term of the individual leaving the School and any emails contained therein will be archived.
g) Important information that is necessary to be kept should be stored separately in the appropriate file(s) not kept in personal folders, archives or inboxes.

Sanctions

Use of the ICT resources at Austin Friars is conditional upon adherence to this Policy. A breach of this policy may be dealt with as a disciplinary matter using the School's usual procedures and may result in a punishment commensurate with the type and seriousness of the breach.

In addition, any breach may result in the School restricting access to School IT systems, temporary or permanent exclusion of pupils or termination of employment for staff. If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it immediately to the Designated Safeguarding Lead. Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing Appendix 1 and returning the signed copy to the School Office; acceptance may be used.

R Scott

Bursar

10 September 2025
****

Reviewed and endorsed by Full Trustees Meeting on:

Next Review by Trustees: Summer Term 2027

Appendices:

1. Acceptance of the ICT Acceptable Use Policy
2. Senior School Online Teaching and Learning Policy

Appendix 1

Acceptance of the ICT Acceptable Use Policy

I understand and accept this acceptable use policy (staff / pupils):

Name: ……

Signature: ……

Date: ……

For younger pupils (below secondary School age)

Name of parent/guardian: ……

Signature: ……

Date: ……

Appendix 2

Senior School Online Teaching and Learning Policy

At Austin Friars, we are proud to deliver our high-quality education. We are also proud that we will be able to do so under exceptional circumstances that may require the school building to close or indeed to provide remote learning should a pupil or member of staff find themselves to be absent in the medium to long term. While Distance Learning does not replicate onsite learning, our teachers can deliver meaningful education to continue with academic syllabus.

This policy summarises the provision of remote learning for pupils, so that there are consistent and well understood expectations of the level of support that will be provided for all concerned.

Remote teaching and learning in case of enforced school/ bubble closure

Pupil/Student expectations:

- Pupils should retain structure to their working day starting with checking school emails and logging-in to Firefly before Zoom lessons begin at 9:05
- Work through any remote tasks set in a timely fashion.
- Complete all set work and hand in on Firefly or email to staff, dependent on instruction
- Communicate with teachers and ask questions if there is an aspect of the work that is not understand or help is required, within normal school hours. Should an email be sent out of school hours, expect that it will be answered the following school day.
- Pupils must sign off that they have completed set work as per teachers' instructions using the Firefly 'submit' function or communicate directly with member of staff
- Pupils may need to photograph work of a visual nature and use the Firefly app to submit this to teachers or use email
- Deadlines must be met; the Heads of School will be informed if they are not.

Teacher expectations:

- Upload teaching materials/lessons to Firefly (email pupils to their school email address if necessary)
- As in the classroom, teachers will use a variety of teaching and learning strategies. Activities will be equivalent in length to the lessons on their timetable. Whatever the task, teachers will be available during scheduled lessons to answer any questions pupils may have. An element of differentiation by outcome is to be expected. Extension tasks may be set if appropriate
- Remote lessons will be shortened to provide several periods of 'off screen' time during the day
- Set tasks on Firefly that include lesson activities and resources. Except for 5th and VI Form, prep will be significantly reduced (to ensure time away from screens)
- Mark and feedback regularly

- Make sure that all resources are available online including scanned pages of textbooks if they are required
- As much as possible, use the usual rewards and sanctions such as merits/credits, and verbal praise/negative incidents
- Teachers should log any absence as 'information' via the intranet

Parents expectations:

- Encourage and support their children's work, including finding an appropriate place to work, checking that set work is completed and ensuring they have some structure to the working day: start and finish times and appropriate breaks
- Ensure that the pupils have the appropriate technology to be able to access and complete the work
- Contact the pupil's Head of School/ DH if there is any concern

NOTES

Further guidance on using online tools Available tools to enrich home learning are:

- Video lessons using Zoom.
- School subscribed software and platforms e.g. Firefly, Mymaths, Kerboodle, Century, ClickView, Mathletics, Educake, GCSEPod
- BBC Bitesize, Twinkl, GeoGebra, PHET, Youtube, Quizlet and Kahoot etc
- Collaboration - many students will find working from home a lonely experience, without the opportunity to collaborate with their friends. The use of Firefly forums can give students a space where they can work together with their friends and their teachers to swap ideas and answer questions.

Feedback - students can continue to receive the feedback they need through online annotation of documents, along with audio feedback, whilst teachers can track their progress and see where support is required.

Safeguarding

This guidance document is supported by the Safeguarding policy at Austin Friars. Specific additions to note:

Parental involvement during video sessions: by bringing staff instruction into the home, the lessons can feel different. The same rules of communication apply as if this were a regularly taught lesson, meaning that the interaction in these lessons are between the teacher and the pupils alone.

Size of groups for home learning. We are aware of the increased level of risk around one-to-one video meetings with pupils, however, there are many reasons why they would be helpful and appropriate. One to-one sessions with students should follow the same guidance as one-to-one conversations in school (e.g. appropriate standards of dress and language) the option for the teacher to record the

teaching session could be used in this instance. Settings options in Zoom also allow background blurring if felt appropriate.

- Staff registering for any software/ platforms, must do so with their school email address.

- Full instructions for Staff on the use of Zoom are available in the Staff Training section on Firefly.
- Where pupils and staff are emailing, the school email address should be used at all times.

Best practice when using Zoom

From 5th April 2020, Zoom forced users to password protect their meeting room. This is an important first step. Other things to do to protect your Zoom space are:

- Always have the 'waiting room' enabled
- Don't allow attendees to join before host
- Mute attendees on joining
- Turn screen sharing facilities for pupils off
- Don't publicise your meeting's link on social media
- Tell people what the Plan B is (ie. if you do have to abort the meeting where will the meeting move to and how people can re-join)
- Turn off your camera and microphone, unless it's needed