Staff Acceptable Use of ICT Agreement

1. The Staff Acceptable Use of ICT Agreement Aims

1.1 Responsible use
Staff are responsible users of the internet, AI models, social media, email and other information and communication technologies for educational, personal and recreational use.

1.2 Protection of the College system
Ashbourne's digital systems (e.g. email, Facebook, website) are protected from deliberate misuse. The College pays particular regard to security against hacking of all descriptions and has installed robust firewall software to prevent unauthorised access to its computer systems.

Examples of threats to the system:
phishing – the fraudulent attempt to obtain sensitive information such as usernames, passwords or credit card details by disguising as a trustworthy entity in an email. Most commonly the fraudsters will pose as a bank asking assistance in resetting login details.

malware or computer viruses – MALicious softWARE (malware) are programs that are harmful to the computer system to which the user belongs. Malware can infect a computer by modifying or deleting data or causing software (e.g. WORD) to work in an unexpected manner. It is commonplace for malware to enter a system because a user has clicked on a link in an email from an untrustworthy source.

compromise of passwords and logins – aside from phishing this can happen if there is a data breach or you reveal your own login details are revealed to another user.

corruption of data – in addition to infection by malware, the system's data may be corrupted because of a failure of our hardware or software. Ashbourne deals with this threat by upgrading both its hardware and software at regular intervals as well as keeping a robust backup of all all data. This means that the College can reinstate the system in minutes should it suffer significant damage.

data encryption – as the name implies encryption translates data into another form so only people with access to a secret key may read it. The College's email facility is provided by Google mail and is automatically encrypted.

Filemaker allows all teachers access to all registers (read-only) but the facility to input and amend data for their own registers only. Using the data protection principle of legitimate interest and the best interests of the student, Ashbourne takes the view that permitting staff to share this specific and limited personal data of students (grades, attendance etc) is a satisfactory arrangement.

Fileserver – another system which holds information about meetings, marketing statistics, contracts etc. which is accessible only by the College's administration team.

1.3 Protection of the Ashbourne community
The protection of staff, students, administration and all others affected by the digital environment at the College.

Ashbourne is committed to enhancing all aspects of education at the College, including the use of and support from digital media.

2. Staff Acceptable Use of ICT Agreement

I understand that I must use ICT in a responsible way, protecting my safety, the safety and security of the ICT systems and the safety and security of other users, especially students.

2.1 Professional and personal safety
2.1.1. I understand that the College will monitor my use of ICT systems, emails and other forms of digital communication.

2.1.2. I understand that the rules set out in this document apply to ICT systems both inside and outside the College.

2.1.3. I understand that the College ICT systems are provided principally for educational purposes and will only use the systems for personal or recreational use within the boundaries set out in this document.

2.1.4. I will not disclose my username or password to anyone else nor will I try to use anyone else's username or password.

2.1.5. I understand that digital recordings (audio and/or visual) of formal and informal meetings and/or lessons by any member of the Ashbourne community, including students, parents/carers and staff, are not permitted.

2.1.6. I will immediately report any illegal, inappropriate or harmful material or incident to the Lead Compliance Officer.

2.2 Professional communications and actions when using the College's ICT systems
2.2.1. I will not access, copy, remove or otherwise alter any other user's files, without consent.

2.2.2. Avoiding the use of aggressive or inappropriate language, I will communicate with others in a professional and courteous manner. I will be tolerant and respectful of the views of others.

2.2.3. If I take or publish images of others, it will only be with their explicit written consent.

2.2.4. I will only use AI models, such as ChatGPT, and social networking sites in College in accordance with the College's policies.

2.2.5. I will not engage in any online activity that will compromise my profession or bring the College into disrepute.

2.2.6. I will only communicate with members of the Ashbourne community using authorised school systems.

2.2.7. If any of the data is breached, I will report immediately to the Lead Compliance Officer.

2.2.8. I will follow the College's guidance, set out in the e-Safety Policy, on delivery of online distance learning.

2.3 Safe and secure access and storage
The College has a responsibility to offer safe and secure access to digital technology. I agree to report any deficiencies in the ICT system to the Lead Compliance Officer.

I will pay particular attention to:

- phishing;
- downloading insecure attachments to emails;
- concealing usernames and passwords (login details);
- uploading software without permission (the danger of malware and viruses).

2.4 Protection against breaches of security and corruption of data:
Do not open attachments from untrustworthy sources

Because of the danger of malware and viruses, I will not open any attachments unless the source is known and trusted.

2.5 Backing up your documents
I understand the importance of continuously backing up my documents.

2.6 Uploading inappropriate material
I will not upload, download or access any material which is illegal (e.g. child sexual abuse images, racist material, adult pornography) or inappropriate or might cause harm or distress to others.

2.7 Supporting the anti-virus firewall
I will not use any software designed to work around the College's firewall or anti-virus programs.

2.8 Uploading large files
I will not try to make large uploads or downloads which might compromise the facility with which others access the digital systems.

2.9 Installing personal software
I will not install any programs or alter the settings on any computer without express consent.

2.10 Abuse of hardware
I will not damage or disable any of the College's ICT equipment or equipment belonging to others.

2.11 Data protection
Sharing personal data

I will not transport, hold, disclose or share personal information as set out in the College's Data Protection Policy. Externally exported personal data should be encrypted.

2.12 Privacy of personal data
I understand the necessity of keeping private any personal data of any member of the Ashbourne community, except when required by law to disclose such to the Designated Safeguarding Lead (DSL) or another appropriate authority.

2.13 Safeguarding trumps data protection
I understand that safeguarding trumps data protection. When children are suffering from, or may be at risk of, suffering significant harm, concerns must always be shared with children's social care or the police.

2.14 Safeguarding and cyberbullying
This is any form of bullying that takes place online or through smartphones and tablets.

I will be alert to instances of cyberbullying and report any to the DSL. Please read our Child Protection and Safeguarding Policy.

2.15 Plagiarism
Plagiarism, including AI-assisted work
I will not use the original work of others in my work without proper credit and will obey the current copyright legislation. I will identify where AI has been used to assist in the production of any work or materials.

Staff Acceptable Use of ICT Declaration
I understand that Ashbourne's Staff Acceptable Use of ICT Agreement applies to the use of the College's ICT systems or hardware inside or outside College. Failure to comply with the agreement may result in disciplinary action.

I have read and understood the terms of the above Agreement as well as the College's e-Safety Policy and agree to use the College's ICT system, my own devices in College and when making communications related to College business, in accordance with these documents.

Staff name:_____

Signature:_____

Date:_____