E-Safety Policy and Acceptable Use Agreement

Full School including EYFS

2025 / 2026

QUI SE VINCIT QUI SE VINCIT QUI SE VINCIT

IPS

Ibstock Place

CO-EDUCATIONAL DAY SCHOOL

IBSTOCK PLACE SCHOOL

E-Safety Policy and Acceptable Use Agreement

Full School including EYFS

Scope

This policy applies to all pupils (age 4 (EYFS) - 18) and staff at Ibstock Place School (hereinafter 'Ibstock' or 'the School').

Roles and Responsibilities

The Governing Body delegates responsibility to the Head for developing and enacting any required "Good Practice" policies. These policies are non-statutory and do not require ratification by the Governing Body. As such, the Head has delegated accountability and responsibility for the operationalisation of this policy to the Director of Strategy and Innovation who ensures the consistent application and implementation of this policy across the School, as detailed under 'Individual Responsibilities' on page 4. Staff should follow the expectations set out in this policy.

Introduction

It is the duty of Ibstock to ensure that every pupil in its care is safe. The same principles apply to the 'digital world' as to the 'real world'. Digital and other computing technologies provide unrivalled opportunities for enhanced learning as a complement to traditional methods, but also pose a number of potential risks to young people. Some of these risks are new and unique to the technologies in question, but the majority are more familiar risks that can manifest virtually. Our pupils are taught how to stay safe in an online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of School include:

- AI Chatbots
- Email
- Social networking sites (Instagram, TikTok)
- Video hosting sites (YouTube, Vimeo)
- Chat apps, including video calling (Snapchat, WhatsApp, Zoom)
- SMS and MMS
- Music/video streaming and downloads, including podcasts (Spotify, Apple Music)
- Gaming sites and console gaming networks (PSN, Xbox Live, Steam)

- Blogs, forums, chat rooms (Reddit, Discord)
- Browser plug-ins
- The proliferation of multiple personal devices: smartphones, tablets, laptops, etc.
- Data privacy and security solutions, often used alongside the above, such as VPNs

The policy reflects the need to raise awareness of the safety issues associated with such technologies as a whole and has been written by the School, having reviewed guidance from the Safer Internet Centre, DfE and Wandsworth Council's guidance.

This policy, supported by the Acceptable Use Agreement (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. The policy will operate in conjunction with other School policies including:

- IT and Computing Policy
- Child Protection and Safeguarding Policy
- Behaviour Management Policy
- Anti-Bullying and Cyber-Bullying Policy
- Staff Handbook (which includes the Staff Code of Conduct)
- PSHE Policy
- Taking, Storing and Use of Images of Pupils Policy
- Pupil Device Rental Agreement / Staff Device Rental Agreement

Whilst exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of these digital technologies.

Ibstock Place School understands the responsibility to educate our pupils on e-safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the Internet and related technologies in and beyond the classroom. The School also understands the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Why Internet Use is Important

We encourage staff and pupils to use the rich information resources available on the School networks and to develop skills to analyse and evaluate such resources. The Internet is an essential element in 21st century life for education, business and social interaction.

The Internet is provided within School to facilitate access to learning resources and enable communication with others for academic and co-curricular purposes. Internet access, because it may lead to any publicly available site in the world, will open classrooms to resources that have not been selected by teachers as appropriate for use by pupils. Just as with home or mobile Internet use, the School cannot accept responsibility for everything that appears online, although it can and does make all reasonable efforts to filter the material available via its network. With this in mind, the School believes that the benefits to pupils from access to learning resources and opportunities for collaboration significantly exceed the potential risks, provided these are appropriately managed.

Policy Overview

This policy applies to all members of the School community, including staff, pupils, parents and visitors who have access to and are users of the School network and any device(s) connected to it. In this policy, 'staff' includes teaching and non-teaching staff, peripatetic staff and contractors. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including contractors.

Both this policy and the Acceptable Use Agreement (for all staff, visitors and pupils) cover both fixed and mobile Internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment), as well as all devices owned by pupils, staff or visitors and brought onto School premises (personal laptops, tablets, smartphones, wearable devices, etc.).

Individual Responsibilities

1. The Governors

The Governors of the School are responsible for the approval of this policy and for reviewing its effectiveness.

2. Head and the Senior Management Team

The Head is responsible for the safety of the members of the School community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the Deputy Head (Pastoral) who is also the School's Designated Safeguarding Lead.

In particular, the roles of the Head and the Senior Management Team are to ensure that:

- staff, in particular the Deputy Head (Pastoral), are adequately trained about e-safety; and
- staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the School.

3. Deputy Head (Pastoral) as E-safety Coordinator

The School's Deputy Head (Pastoral) is also the Deputy Designated Safeguarding Lead and acts as the School's E-safety Coordinator. The Deputy Head (Pastoral) is responsible to the Head for the day-to-day issues relating to e-safety, including filtering and monitoring. The Deputy Head (Pastoral) has responsibility for ensuring this policy is upheld by all members of the School community and works with the Director of Digital Strategy, the Head of Digital Innovation and Learning and the Head of IT to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and Wandsworth MASH team. The Deputy Head (Pastoral) leads on the annual review of filtering and monitoring systems.

4. Technical Staff

The School's technical staff includes the Head of IT, the IT Technicians, and the Data Manager, all managed by the Director of Digital Strategy. Collectively, they have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast of technical developments. The Head of IT is principally responsible for the security of the School's network and hardware. He monitors the use of the Internet and emails, maintains content filters, and will report inappropriate usage to the Deputy Head (Pastoral). The Data Manager is responsible for the security of the School's data. Judicium Education is the School's designated Data Protection Officer. Collectively, the technical team is also responsible for training the School's teaching and administrative staff in the use of digital and other computing technologies.

5. Teaching and support staff

All staff are required to read and abide by the IT and Computing Policy and the Acceptable Use Agreement before accessing the School's systems. The Acceptable Use Agreement governs staff conduct for both safeguarding and cybersecurity purposes.

6. Pupils

Pupils are responsible for using the School IT systems in accordance with the Acceptable Use Agreement and for informing staff if they see IT systems being misused.

Education and Training

1. Staff: Awareness and Training

New teaching and administrative staff receive information on the School's e-safety and Acceptable Use policies as part of their induction.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety as part of their safeguarding briefing on arrival at School and through regular (at least annual) safeguarding updates. This includes their duties with regard to filtering and monitoring software.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School e-safety procedures. These behaviours are summarised in the Acceptable Use Agreement which must be electronically signed and returned before use of digital technologies in School.

Teaching staff incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the School's Deputy Head (Pastoral). A full report should also be added to My Concern (the School's cloud based safeguarding software).

2. Pupils: E-Safety in the Curriculum

The School provides opportunities to teach about e-safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside School will also be tackled in PSHE and Tutorial activities.

Pupils are taught about their e-safety responsibilities and to look after their own online safety. They are taught about recognising the risks of online sexual exploitation, stalking and grooming and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Deputy Head (Pastoral) or any other member of staff at the School. The School's filtering and monitoring systems are explained annually to pupils as part of the assembly programme, as well as being documented in the Acceptable Use Agreement and the Pupil Device Rental Agreement.

Pupils are also taught about relevant laws applicable to using the Internet, such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through the School's Tutorial programme.

Pupils are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-Bullying and Cyber-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach the Deputy Head (Pastoral), as well as parents, peers and other School staff for advice or help if they experience problems when using the Internet and related technologies.

Encouraging and educating pupils on the safe use of the Internet is achieved in the following ways:

- E-safety information is provided to all pupils as part of the pastoral programme
- Parents are invited to regular Digital Awareness presentations and have access to a wealth of resources through the Teen Tips Wellbeing Hub
- New pupils to the School are addressed by the Deputy Head (Pastoral) on the first day
- E-safety is embedded into the academic curriculum with teachers guiding pupils towards safe online activity.

3. Parents

The School will always contact parents if it has any concerns about pupils' e-safety behaviour and likewise it hopes that parents will feel able to share any concerns with the School.

The School expects parents' support regarding safe Internet use and will draw their attention to it when access to the Parent Portal is made available to them prior to their child starting at the School via the Acceptable Use Agreement that they are also required to acknowledge and accept.

Policy Statements

1. Use of School and Personal Devices

a) Staff

Staff are required to read, sign and adhere to the Staff Device Rental Agreement when issued with a School-owned device. School devices assigned to a member of staff as part of their role have a password or device lock so that unauthorised people cannot access the content. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Staff are trained on appropriate data storage locations to ensure that sensitive or personal data are not present for longer than needed on the physical storage of the device, instead using secure cloud storage options where appropriate. In the event that a School device is lost or stolen, staff first inform the Director of Digital Strategy and the Head of IT, who will then investigate the potential risks and, where possible, clear data from the device remotely. Staff are not permitted to install additional software on or make other such changes to School devices, which operate within a centrally managed software environment. Requests for subject-specific software are sent in the first instance to the requester's line manager and then to the Director of Digital Strategy for review.

Staff are permitted to bring in personal Smart Phones for their own use. Staff are referred to the Bring Your Own Device (BYOD) guidance in the IT and Computing Policy for further guidance on the use of non-School owned electronic devices within school grounds. Staff use a dedicated WiFi network for this purpose, which is linked to the School's web filter.

Staff should not give their personal contact details to pupils, including email addresses, home or mobile telephone numbers, unless the need to do so is agreed with the Senior Management Team and parents, guardians or carers. Staff are required to adhere to guidance outlined in the School's Child Protection and Safeguarding Policy.

Any digital communication between a member of staff and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through Internet platforms not administered by the School, even where such platforms have an educational purpose. Further information can be found in the Social Media policy.

b) Pupils

Users require Ibstock domain credentials to access the WiFi networks so we can ensure that only enrolled staff or pupils are active on the network. All access is subject to acceptance of the Acceptable Use Agreement.

In addition, extra firewall restrictions are imposed via DHCP to separate and secure devices. These include bandwidth and routing policies.

Pupils in most Senior School year groups are issued with a School-owned Microsoft Surface device. All activity on the device is subject to the School's filtering and monitoring systems (detailed further below) and conduct while using the device is governed by the Acceptable Use Agreement and Pupil Device Rental Agreement. In particular, pupils acknowledge in signing the Agreement that all of their online activity is subject to the School's filtering and monitoring policies and that evidence such as screenshots of their activity will be collected when inappropriate use is detected.

Smartphones and other personal mobile devices brought into School are the sole responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of pupil smartphones or other devices. Lower and Middle School pupils are not allowed to use personal mobile devices on campus before 4pm.

Mobile devices must not be taken into examinations. Pupils found in possession of a mobile device during an examination will be reported to the appropriate examining body. This may result in the withdrawal of the pupil from either that examination or all examinations.

If a member of staff suspects a message, text or similar, may contain inappropriate content it should be referred to the DSL. In particular, the School requires pupils to ensure that their use of personal mobile devices for both academic and co-curricular work complies with this policy and the Acceptable Use Agreement.

2. Use of the Internet and Email

a) Staff

Staff must use social networking sites with caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the School. Staff are required to follow the advice contained within the Staff Code of Conduct and the Social Media Policy for Staff.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that email communications through the School network and staff email addresses are monitored and archived. The School can also trace messages sent via other administered platforms, such as Microsoft 365 (Teams, etc.) and Zoom.

Staff must immediately report to the Deputy Head (Pastoral) or IT staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Director of Digital Strategy or Head of IT.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Ibstock Place School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or
- do anything that could be considered discrimination against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender identity, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.

b) Pupils

All pupils are issued with their own School email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all schoolwork. Pupils should be aware that email communications through the School network and School email addresses are monitored.

There is industry standard antivirus and firewall protection on our network. Spam emails and suspicious attachments will be blocked automatically by the email system. If this causes problems for schoolwork/research purposes, pupils should contact the IT team for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the Deputy Head (Pastoral), IT staff or another member of staff.

The School expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Deputy Head (Pastoral) or another member of staff. Deliberate access to any inappropriate materials by a pupil will be dealt with under the School's Behaviour Policy. Pupils should be aware that all Internet usage via the School's systems and WiFi network is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for schoolwork/research purposes, pupils should contact the Deputy Head (Pastoral) or IT staff for assistance.

3. Data Storage and Processing

The School takes its compliance with Data Protection Law seriously. Please refer to the Information Security and Data Protection Policy, the Acceptable Use Agreement and the School's Privacy Notice for further details.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be reported to the Data Protection Officer and a member of the Senior Management Team immediately.

4. Password Security

Pupils and staff have individual School network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and staff and must use a strong password. They are asked not to write passwords down and advised not to share passwords with anyone else.

5. Safe Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet (e.g., on social media sites).

Staff, pupils, parents and visitors must follow this policy, the Taking, Storing and Use of Images of Pupils Policy, the Acceptable Use Agreement and the Information Security and Data Protection Policy concerning the sharing, distribution and publication of images of pupils.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Consent will be obtained before photographs are published on the School's public facing websites or in School publications (see the Taking, Storing and Use of Images of Pupils Policy, Parent Contract and Privacy Notice for more information).

6. Misuse

Ibstock Place School will not tolerate illegal activities or activities that are inappropriate in a School context and will report illegal activity to the police and/or Children's Services. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the School's policies and procedures, in particular the Child Protection and Safeguarding Policy.

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying and Cyber-Bullying Policy.

7. Complaints

As with all issues of safety at School, if a member of staff, a pupil or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it.

Complaints should be addressed to the Deputy Head (Pastoral) in the first instance, who will liaise with the School's Senior Management Team and undertake an investigation where appropriate.

Incidents of or concerns around e-safety will be recorded and reported to the School's Deputy Head (Pastoral) and Designated Safeguarding Lead or one of the Deputy DSLs in his/her absence, in accordance with the School's Child Protection and Safeguarding Policy.

8. School Approach to Managing Internet Access (incl. Filtering and Monitoring)

Direct Internet Links from School

The School uses a Sophos XG Firewall solution.

File Type Block

End Users cannot download potentially dangerous file types, including batch and executable files through the firewall.

Malware/Virus protection

The Sophos XG Firewall and NGFW assess all downloadable files for viruses and malware before delivering to the user. Sophos end point protection is used as a second level of protection.

Filtering

The School uses Sophos maintained categorisations on the Sophos XG Firewall. These are updated automatically from Sophos Labs, a 24/7 security centre working around the globe to combat Internet threats. The suitability of this filtering solution is reviewed annually as part of the Filtering and Monitoring Annual Review process, signed off jointly by the Director of Digital Strategy, the Deputy Head (Pastoral) and the Digital Link Governor(s).

From these categories we build our rulesets to block undesirable websites. These include: *Anonymisers; Botnet; Criminal Activities; Gambling; Hate/Discrimination; Illegal Drugs; Malicious; Obscene/Tasteless; Pornography; Phishing; Spyware/Adware; Violence, etc.*

SSL Inspection

School networked computers are configured so that any encrypted Internet traffic to a secure site (https://) can also be inspected for hidden threats. At the same time, SSL scanning is also used to monitor Internet usage and ensure that School policies are adhered to.

Application Traffic

Internet traffic that is not browser-based but app-based is monitored by our Firewall. All user activity is recorded and monitored. Where possible, undesirable apps are blocked, such as peer-to-peer file sharing, tunnelling and proxy-avoidance services.

Monitoring

A visual monitoring programme called Senso is used to monitor all School-owned devices used by pupils. Senso flags language and imagery that contravene the Acceptable Use Agreements and notifies classroom teachers of these infractions immediately. In addition, email alerts highlighting infractions of particular concern/severity are sent to the Deputy Head (Pastoral), the Director of Digital Strategy, the Head of IT, and the Heads of Section. Weekly summaries of Senso flags are produced for this same group of stakeholders and are regularly reviewed. Teaching staff cannot access Senso outside of working hours or away from the School campus. The suitability of this monitoring solution is reviewed annually as part of the Filtering and Monitoring Annual Review process, signed off jointly by the Director of Digital Strategy, Director of Safeguarding and the Digital Link Governor(s).

Comprehensive Reporting

The School generates monthly usage reports from our Sophos XG Firewall. These provide Internet data usage and policy violation reports on users. These reports are published to the IT Department.

We also use FastVue reporting software for the Firewall. This provides live and historical browser-based traffic reporting. It is published through a user-friendly web interface. These reports are accessible to the Head of IT for dissemination to members of the SMT where required.

Email

Each user is provided with an individual email address which is integrated with Active Directory to provide traceable activity and granular security settings. All user mailboxes are stored on the cloud, within the secure Microsoft 365 environment. Web-based email (Outlook Web Access) incorporates browser security and keeps email on the Microsoft 365 servers rather than diverse local mailboxes, avoiding the attendant dangers thereof.

Email filtering is done by Barracuda Email security services, which checks every external email for viruses/malware, inappropriate language and common spam keywords. Suspicious or malicious attachments are sent to a quarantine that can be accessed by the Head of IT and released to the recipient if necessary. Barracuda Sentinel is used to detect spear phishing, account takeover and domain fraud attacks.

Client Machines

We use both the Windows 10 and 11 operating systems with monthly WSUS managed patch rollouts. We have policy-implemented screen locks and have installed secure browsers with minimal plug-ins. All client machines have antivirus updated as soon as a newer definition is released. This is centrally monitored and managed by a Sophos Enterprise Console, which provides remote diagnostics, repairs and regular reports.

Users cannot generally install programs onto School computers and must contact the IT Department if this is required. Some commonly requested and pre-approved programs are available via the 'Company Portal' tool. IT staff take responsibility for updating programs known to have vulnerabilities (Adobe Reader, Flash, etc.).

4G and 5G Accessibility

The School recognises that it cannot manage direct Internet access from mobile devices. In order to ensure that everyone in our community is using the Internet safely and appropriately, e-safety education, codes of conduct and behaviour and Acceptable Use Agreements are established for staff and pupils alike.

The use of cellular technology is restricted to Sixth Form pupils or, for other age groups, to 'after school' use post-4pm. Sanctions are in place for breaches of the School's rules and code of conduct.

Queries

Queries on this policy should be directed to the Director of Digital Strategy.

Review and Verification

This policy is reviewed annually by the Director of Digital Strategy.

Appendices

Acceptable Use Agreements and Glossary of Terms are appended to this policy.

Appendix A.1

IBSTOCK PLACE SCHOOL

Staff and Visiting Teacher Acceptable Use Agreement

Equipment, Security and Privacy, Internet and Email
and IT Network Policy

Name: ……………………………………………………………………………………

Department: ………………………………………………………………………………

Introduction

The School has provided IT facilities for the use of staff and visiting teachers in the course of their professional duties and, in turn, for the education of our pupils. The purpose of this agreement is to set out the conditions of use by staff and visiting teachers of the School's IT and Computing facilities.

Equipment:

I agree that I shall not:

- install, attempt to install, or store programs of any type on the computers without the agreement of the Head of IT.
- attempt to disassemble or repair any equipment but, if encountering malfunction, always refer problems of a technical nature to the IT Staff.
- use the computers for personal commercial purposes, e.g. buying or selling goods.
- open files brought in on removable media (such as USB flash drives, CDs, etc.) or via email/download until they have been checked with antivirus software by the IT team and found to be virus free.

- connect, or attempt to connect, any equipment to the network (e.g. mobile devices, laptops, tablets etc.) either wired or wirelessly without the agreement of the Head of IT.
- eat or drink near IT equipment.
- use the School network for creating any materials which are unlawful, obscene, abusive or extremist/propagandist.
- keep School equipment in my possession after the return date specified by the IT Staff.
- store personal or sensitive data relating to the School or its community on the physical storage of any device for longer than is strictly necessary, if at all.

Security and Privacy:

I agree that I:

- shall change my domain login password the first time I log on.
- shall not disclose my password to others, or use passwords intended for the use of others. I understand I may only use a computer whilst logged in with my own username and password. If a computer is logged on by another person and I wish to use it but I cannot find that person, I agree to log that person off before proceeding. If in doubt I shall contact the Head of IT or an IT Technician.
- shall not disclose Ibstock wireless network or other passwords to any other person.
- shall not store any Ibstock or pupil data on removable media (such as USB flash drives, external HDDs or SSDs etc.) without the prior permission of SMT and shall seek permission anew for each instance of using removable media.
- shall not share, save or download any Ibstock or pupil data other than when strictly necessary and, once such data is no longer required or once I am no longer contracted by School, I will take all reasonable steps to delete any versions I have made.
- shall adhere to data storage good practices relating to the intellectual property of the School, such as storing shared resources in shared locations accessible by all appropriate parties (e.g. SharePoint) and, before ending my contractual relationship with the School, that I shall transfer any intellectual property kept in personal spaces (e.g. OneDrive) to a shared location or to a colleague.
- shall not knowingly obtain or attempt to obtain unauthorised access to any part of any network, or any information contained on such a network, including the School network. I understand that hacking is a criminal offence and can be grounds for dismissal.
- understand that access to data on the School network is provided to me solely for the execution of my professional duties and belongs to the School; School data may not, in any form or on any media, be used, distributed or in any way passed to another party for any reason whatsoever.
- shall not use the computers in a way that harasses, endangers, harms, offends or insults others.
- shall not attempt to bypass any security in place on School devices or attempt to alter any related settings.
- shall inform the Head of IT immediately if I have accidentally read, downloaded or been sent inappropriate material, including personal information about someone else
- understand that, for my own protection and that of others, any activity I undertake on a School device and/or through the School network, including my files, my use of the Internet

and my email communications, is subject to the School's filtering and monitoring policies and that reports on my usage may be shared externally (e.g. with child protection or law enforcement agencies) as deemed appropriate by the Head.

- Shall not make use of proxies or VPNs to circumnavigate the filtering in place on the school network

Internet and Email:

I agree that I:

- shall not access the Internet or use email unless for School activities.
- shall not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive or propagandist.
- shall respect the work and ownership rights of people both within and beyond the School community, including abiding by copyright laws.
- shall not engage in activities over the Internet that inappropriately consume bandwidth (e.g. game or video streaming, video calling) unless directly related to School activities.
- shall not bring the School into disrepute through my use of email, the Internet or any related services.
- shall never open attachments to email messages or click on unsolicited links unless I am confident they come from a source that is known and trusted; I understand these may trigger viruses or other programs which may cause damage to my computer and/or the network.
- understand that malicious emails and files often come from seemingly credible sources, such as an email address very similar to the genuine email address of a parent, and as such I agree to thoroughly scrutinise incoming emails and files, checking against the iSAMS database where necessary, and to consult the Head of IT immediately if I have a concern.
- understand that sending or receiving email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies but is not limited to any material of a sexual, vulgar, violent, racist or extremist/propagandist nature; I shall always report messages of these kinds to the Head of IT.
- am responsible for any data that may be stored locally on a personal device as a result of using a personal mail client (e.g. Apple Mail on an iPhone) and must store and dispose of such data in line with the terms of this agreement and all other School policies.
- will delete, before ending my contractual relationship with the School, any Ibstock emails and attachments from my personal devices that have been locally saved as a result of using a personal mail client.
- have read the information in the Staff Handbook about corresponding with pupils, parents and others, and the procedures which must be followed.

I have read and understood these conditions and I agree to abide by them at all times.

Name:..

Email address: ....@ibstockplaceschool.co.uk

Signature:.. Date: ....

Staff may not have access to the School's email, Internet and network facilities unless this signed contract is returned to the Head of IT. If any member of staff fails to observe these conditions, access to the network may be withdrawn, and you may be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.

Appendix A.2

IBSTOCK PLACE SCHOOL

IT Use Pupil Agreement
(Senior School)

Equipment, Security and Privacy, Internet and Email
and IT Network Policy

Introduction

We want all pupils at Ibstock Place School to enjoy using the School network and to become proficient in drawing upon it both during your time at School and as a foundation for your further education and career. Computers, networks and related devices are provided and maintained for the benefit of all pupils, who are encouraged to use and enjoy these resources and ensure they remain available to all. Pupils are responsible for their conduct on the Internet, just as they are in a classroom or a school corridor. The purpose of this agreement is to set out the rules that must be followed by users of the network.

Rules

Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc) until they have been checked with antivirus software and been found to be clean of viruses.
- Do not connect or attempt to connect any device(s) to the network (smartphones, wearables, laptops, tablets etc.) either by wire or wirelessly.
- Do not eat or drink near computer equipment.
- Do not use the School network or devices for creating any materials which are unlawful, obscene, abusive or in any other way contravene the School's behaviour policies.

Security and Privacy

- You must change your password the very first time you log on.
- Do not disclose your password to others, or use passwords intended for the use of others. You may only use a computer whilst logged in with your own username and password.
- Do not knowingly obtain or attempt to obtain unauthorised access to any part of any network, or any information contained on such a network, including the School network. Hacking is a criminal offence and a serious breach of School rules.
- Never tell anyone you meet on the Internet your home address, your telephone number, your School's name, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.

- You must not attempt to bypass security in place on the computers or attempt to alter any settings; this includes the use of proxy sites, VPNs and browser plug-ins, attempted installation of which is a serious breach of School rules.
- You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.
- For your own protection and that of others, staff may read/review all files, Internet use and email communications to ensure that users are using the system responsibly; this applies to activity both on School devices and on all other devices connected to the Ibstock network.

Internet and Email

- Do not access the Internet or use email unless for study, or for School authorised/supervised activities. Social media and direct messaging ("DMs") of all kinds are not allowed unless directly required by a teacher supervising the activity.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the School, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet and never arrange to meet anyone you encounter online. Inform a teacher or your parent/guardian if anyone suggests this to you.
- The same rules apply to your online conduct as to your physical conduct in School: be polite during online discussions and appreciate that other users might have different views from your own.
- You must not bring the School into disrepute through your use of email, the Internet or related services. Impersonating the School using fake accounts is strictly prohibited.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other harmful programs. Be aware that criminals often use email addresses designed to look very similar to the real email address of someone you know.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.
- Do not at any time use the School network or a School device to play games. The definition of a 'game' is always at the discretion of the supervising member of staff.

When you have returned this agreement, signed, your account will be enabled. Your Tutor or Head of Year will explain how to access it. Please note your username below so that you can do so.

AGREEMENT

NAME: .... YEAR GROUP: ....

Please note that your username is: ....

(one word, no spaces or punctuation)

and your Ibstock email address is: ....@ibstockplaceschool.co.uk

I agree to observe the conditions of this agreement as outlined above.

Signed (pupil):.. Date:...........................

Signed (parent):.. Date:...........................

A copy of this agreement is available for future reference on the School Intranet.

Pupils may not have access to the School's Email, Internet and Network facilities unless this signed agreement is returned to the Head of IT. If any pupil violates these provisions, access to the network may be withdrawn, and you may be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.

Appendix A.3

IBSTOCK PLACE SCHOOL

IT Use Pupil Agreement
(Prep School)

NAME .... FORM ....

School Username: ....

School Email Address: .... @ibstockplaceschool.co.uk

Please read the information below and ask your teacher if you do not understand it.
You must follow these guidelines if you use IT equipment at School.

- I shall always use what I have learned about e-safety to keep myself safe and shall tell a teacher if something makes me worried or unhappy.
- I shall use School computers for schoolwork and not to upset or be rude to other people.
- I shall only use my School email account (which ends in @ibstockplaceschool.co.uk) in School.
- I shall not open any email attachments without checking with an adult.
- I shall only go on websites and search engines that my teacher tells me to.
- I shall tell my teacher straight away if I go on a website by mistake.
- I shall tell a teacher straight away if I see a website I did not try to open, or receive emails from people I do not know.
- I shall look after school IT equipment and tell a teacher straight away if something is broken or not working properly.
- I shall not try to download or install any software on school computers.

- I shall only use the username and password I have been given and I shall keep them secret.

- I shall save only schoolwork on the School network and shall check with my teacher before printing.

- I shall log off a computer when I have finished using it.

I understand that all of my work and Internet activity on school IT equipment can be seen by teachers and that they will sometimes check that I am following these guidelines.

I understand that I must follow these rules. If I do not, my use of IT equipment at School may be stopped.

Pupil's Signature: ....

I have discussed this document with my child and agree to his/her use of IT equipment at School according to this agreement.

Parent's Signature: .... Date: ....

Appendix B.1

Glossary of Terms

The definitions given below apply throughout this policy, its appendices and in all other Ibstock materials.

The dynamic nature of this field means that the nuance to these terms – and therefore their usage, particularly spoken usage – is frequently shifting but, for the avoidance of doubt, the definitions below take precedence until such time as the policy is reviewed.

App	A piece of software. Most commonly used in the context of smartphones and tablets, where such software is downloaded and maintained via an "app store" rather than as a one-off download or installation from a CD/DVD. Desktop and laptop PCs are increasingly moving towards this model of software management.
Cloud storage	Data storage held on 3rd party servers and accessed via the Internet, such as Microsoft OneDrive or Google Drive
Computer Science	An academic discipline taught at Ibstock and elsewhere
Computing	A broad term covering all use of computers, including programming, engineering, networking etc.
Device	A piece of equipment capable of performing computing tasks; can be fixed or mobile, School-owned or personal
Digital	An umbrella term that incorporates all computing activities as well as other networked or Internet services. Synonymous with "IT" except generally used to emphasise the customer or user experience, rather than the technical and infrastructural inputs.
Hardware	The physical manifestation of computing devices and/or components thereof
ICT	"Information and Communication Technology" or, erroneously, "Information and Computing Technology". Intended to a be a broader term than IT, encompassing external infrastructure such as telecommunications networks. **Use of this term is discouraged due to its ambiguity.**
IT	"Information technology", used as an umbrella term for all computing activities and networked services. Unlike "digital", IT generally emphasises the infrastructural and technical inputs rather than the user or customer experience.
Local storage	Storing data on a physical drive within the Ibstock network, either on a specific device (Hard Disk Drive, Solid State Drive) or on the network server (a "shared drive")
Network	The combined IT equipment of the School and the services and infrastructure that enable this interconnection, including as an entry-point to the Internet for both School and personal devices.
Physical storage	Data storage that is not accessed via the Internet, such as a Hard Disk Drive, Solid State Drive, a CD/DVD or a USB Drive

Platform	A digital service run from 3rd party servers usually accessed via the Internet, e.g. Firefly. Whilst technically a form of “software”, this term is generally treated as distinct from "software" as a platform does not need to be specifically installed on an Ibstock device.
Software	The virtual manifestation of computer activity, encompassing the programs and other operating processes run by a device or across a network. While this term technically includes “platforms”, software most often refers to programs that need to be installed, as opposed to “platforms”, which generally run without installation via the Internet.