E-Safety Policy

Prep School including EYFS

2025/2026

Ibstock Place

IBSTOCK PLACE SCHOOL

E-Safety Policy

Prep School including EYFS

Scope

This policy applies to all Prep pupils (including EYFS) 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 Prep School Co-Heads and DSL, who ensure the consistent application and implementation of this policy across the School. Staff should follow the expectations set out in this policy.

1. Introduction

All pupils and staff, academic and non-academic, sign the ICT Users Agreement Form before being given access to the School's files. It aims to provide clear guidance on how to minimise risks. It is linked to the following policies:

- Child Protection and Safeguarding
- PSCHE
- Staff Code of Conduct
- Behaviour Management
- Anti-bullying and Anti-Cyberbullying
- ICT Acceptable Use (staff and pupils)
- Social Media Policy for Staff
- Mobile Devices for Pupils
- Data Protection and GDPR
- Prep Remote Learning
- EYFS Policy
- Computing

At Ibstock, there is a clear, progressive online safety education programme as part of the Computing curriculum and PSCHE curriculum. This aims to build resilience, critical thinking skills and behaviours appropriate to the age and experience of pupils. Pupils are regularly reminded about their responsibilities, and messages are reinforced as part of pastoral activities, particularly in PSCHE lessons.

2. Curriculum Overview

Computing:

IBSTOCK PLACE PREP SCHOOL
LONG-TERM PLANNING
COMPUTING 2024-2025

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Prep 1	Technology Around Us -E-safety - Technology in our classroom -Using technology -Developing mouse skills -Using a computer keyboard - Developing keyboard skills	Creating Media - How can we paint using computers? - Using shapes and lines - Making careful choices -Why did I choose that? - Painting all by myself	Programming A - Buttons - Directions - Forwards and backwards - Four directions - Getting there -Routes	Data and Information - Label and match - Group and count -Describe an object -Making different groups - Comparing groups - Answering questions	Creating Media- Digital Writing - Exploring the keyboard - Adding and removing text -Exploring the toolbar - Making changes to text	Programming B -Exploring the keyboard - Adding and removing text - Exploring the toolbar - Making changes to text -Explaining my choices - Pencil or keyboard

	– Using a computer responsibly	– Comparing computer art and painting			– Explaining my choices – Pencil or keyboard	
Prep 2	IT around us E-safety Lesson 1 What is IT? Lesson 2 IT in school Lesson 3 IT in the world Lesson 4 The benefits of IT Lesson 5 Using IT safely Lesson 6 Using IT in different ways	Creating Media Lesson 1 Taking Photographs Lesson 2 Landscape or portrait? Lesson 3 What makes a good photograph? Lesson 4 Lighting Lesson 5 Effects Lesson 6 Is it real?	Programming A Lesson 1 Giving instructions Lesson 2 Same but different Lesson 3 Making predictions Lesson 4 Mats and routes Lesson 5 Algorithm design Lesson 6 Debugging	Data and Information Lesson 1 Counting and comparing Lesson 2 Enter the data Lesson 3 Creating pictograms Lesson 4 What is an attribute? Lesson 5 Comparing people Lesson 6 Presenting information	Creating Media Lesson 1 How music makes us feel Lesson 2 Rhythms and patterns Lesson 3 How music can be used Lesson 4 Notes and tempo Lesson 5 Creating digital music Lesson 6 Reviewing and editing music	Programming B Lesson 1 Comparing tools Lesson 2 Joining blocks Lesson 3 Make a change Lesson 4 Adding sprites Lesson 5 Project design Lesson 6 Following my design
Prep 3	Connecting Computers E-safety 1. Computing systems and networks – Connecting computers	Creating Media Lesson 1 Can a picture move? Lesson 2 Frame by frame	Programming A Lesson 1 Introduction to Scratch Lesson 2 Programming sprites	Data and Information Lesson 1 Yes or no questions Lesson 2 Making groups Lesson 3 Creating a	Creating Media Lesson 1 Words and pictures Lesson 2 Can you edit it?	Programming B Lesson 1 Moving a sprite Lesson 2 Maze movement

	2. Creating media - Stop-frame animation 3. Programming A - Sequencing sounds 4. Data and information – Branching databases 5. Creating media – Desktop publishing 6. Programming B - Events and actions in programs	Lesson 3 What's the story? Lesson 4 Picture perfect Lesson 5 Evaluate and make it great! Lesson 6 Lights, camera, action!	Lesson 3 Sequences Lesson 4 Ordering commands Lesson 5 Looking good Lesson 6 Making an instrument	branching database Lesson 4 Structuring a branching database Lesson 5 Using a branching database Lesson 6 - Two ways of presenting information	Lesson 3 Great template! Lesson 4 Can you add content? Lesson 5 Lay it out Lesson 6 Why desktop publishing?	Lesson 3 Drawing lines Lesson 4 Adding features Lesson 5 Debugging movement Lesson 6 Making a project
Prep 4	Connecting Computers E-Safety Lesson 1 Connecting networks Lesson 2 What is the Internet made of? Lesson 3 Sharing information Lesson 4 What is a website? Lesson 5 Who owns the web?	Creating Media Lesson 1 Digital recording Lesson 2 Recording sounds Lesson 3 Creating a podcast Lesson 4 Editing digital recordings Lesson 5 Combining audio	Programming A Lesson 1 Programming a screen turtle Lesson 2 Programming letters Lesson 3 Patterns and repeats Lesson 4 Using loops to create shapes	Data and Information Lesson 1 Answering questions Lesson 2 Data Collection Lesson 3 Logging Lesson 4 Analysing data Lesson 5 Data for answers	Creating Media Lesson 1 Changing digital images Lesson 2 Changing the composition of images Lesson 3 Changing images for	Programming B Lesson 1 Moving a sprite Lesson 2 Maze movement Lesson 3 Drawing lines Lesson 4 Adding features Lesson 5 Debugging movement

	Lesson 6 Can I believe what I read?	Lesson 6 Evaluating podcasts	Lesson 5 Breaking things down Lesson 6 Creating a program	Lesson 6 Answering my question	different uses Lesson 4 Retouching images Lesson 5 Fake images Lesson 6 Making and evaluating a publication	Lesson 6 Making a project
Prep 5	Systems and Searching E-safety Lesson 1 Systems Lesson 2 Computer systems and us Lesson 3 Searching the web Lesson 4 Selecting search results Lesson 5 How search results are ranked Lesson 6 How are searches influenced	Creating Media Lesson 1 What is video? Lesson 2 Filming techniques Lesson 3 Using a storyboard Lesson 4 Planning a video Lesson 5 Importing and editing video Lesson 6 Video evaluation	Programming A Lesson 1 Connecting Crumbles Lesson 2 Combining output components Lesson 3 Controlling with conditions Lesson 4 Starting with selection Lesson 5 Drawing designs Lesson 6 Writing and testing algorithms	Data and Information Lesson 1 Creating a paper-based database Lesson 2 Computer databases Lesson 3 Using a database Lesson 4 Using search tools Lesson 5 Comparing data visually Lesson 6 Databases in real life	Creating Media Lesson 1 The drawing tools Lesson 2 Creating images Lesson 3 Making effective drawings Lesson 4 Layers and objects Lesson 5 Manipulating objects Lesson 6 Create a vector drawing	Programming B Lesson 1 Exploring conditions Lesson 2 Selecting outcomes Lesson 3 Asking questions Lesson 4 Planning a quiz Lesson 5 Testing a quiz Lesson 6 Evaluating a quiz

Prep 6	Communication and collaboration E-Safety Lesson 1 Internet addresses Lesson 2 Data packets Lesson 3 Working together Lesson 4 Shared working Lesson 5 How we communicate Lesson 6 Communicating responsibly	Creating Media Lesson 1 What makes a good website? Lesson 2 How would you lay out your web page? Lesson 3 Copyright or CopyWRONG? Lesson 4 How does it look? Lesson 5 Follow the breadcrumbs. Lesson 6 Think before you link!	Programming A Lesson 1 Introducing variables Lesson 2 Variables in Programming Lesson 3 Improving a game Lesson 4 Designing a game Lesson 5 Design to code Lesson 6 Improving and sharing	Data and Information Lesson 1 What is a spreadsheet? Lesson 2 Modifying spreadsheets Lesson 3 What's the formula? Lesson 4 Calculate and duplicate Lesson 5 Event planning Lesson 6 Presenting data	Creating Media Lesson 1 Introduction to 3D modelling Lesson 2 Modifying 3D objects Lesson 3 Make your own name badge Lesson 4 Making a desk tidy Lesson 5 Planning a 3D model Lesson 6 Make your own 3D model	Programming B Lesson 1 The micro: bit Lesson 2 Go with the flow Lesson 3 Sensing inputs Lesson 4 Finding your way Lesson 5 Designing a step counter Lesson 6 Making a step counter

PSCHE

During PSCHE lessons, pupils are likely to talk about technology in conjunction with their everyday actions and interactions. The Prep 5 and Prep 6 'Relationships' topic delves into this more thoroughly, focusing on the use of digital media, including the dangers of it and using it wisely. Pupils are taught about their digital footprint and taking responsibility when using different digital platforms.

Age Group	Being Me In My World	Celebrating Difference	Dreams and Goals	Healthy Me	Relationships	Changing Me
Ages 8-9	Being part of a class team Being a school citizen Rights, responsibilities and democracy (school council) Rewards and consequences Group decision-making Having a voice What motivates behaviour	Challenging assumptions Judging by appearance Accepting self and others Understanding influences Understanding bullying Problem-solving Identifying how special and unique everyone is First impressions	Hopes and dreams Overcoming disappointment Creating new, realistic dreams Achieving goals Working in a group Celebrating contributions Resilience Positive attitudes	Healthier friendships Group dynamics Smoking Alcohol and vaping Assertiveness Peer pressure Celebrating inner strength	Jealousy Love and loss Memories of loved ones Getting and Falling Out Girlfriends and Boyfriends Showing appreciation to people and animals	Being unique Having a baby Girls and puberty Confidence in change Accepting change Preparing for transition Environmental change
Ages 9-10	Planning the year ahead Being a citizen Rights and responsibilities Rewards and consequences How behaviour affects groups Democracy, having a voice, participating	Cultural differences and how they can cause conflict Racism Rumours and name-calling Types of bullying Materials wealth and happiness Enjoying and respecting other cultures	Future dreams The importance of money Jobs and careers Dream job and how to get there Goals in different cultures Supporting others (charity) Motivation	Smoking including vaping Alcohol and vaping Alcohol and anti-social behaviour Emergency aid Body image Relationships with food Healthy choices Motivation and behaviour	Self-recognition and self-worth Building self-esteem Safer online communities Rights and responsibilities online Online gaming and gambling Reducing screen time Dangers of online grooming SMARRT internet safety rules	Self- and body image Influence of online and media on body image Puberty for girls Puberty for boys Conception (including IVF) Growing responsibility Coping with change Preparing for transition
Ages 10-11	Identifying goals for the year Global citizenship Children's universal rights Feeling welcome and valued Choices, consequences and rewards Group dynamics Democracy, having a voice Anti-social behaviour Role-modelling	Perceptions of normality Understanding disability Power struggles Understanding bullying Inclusion/exclusion Differences as conflict, difference as celebration Empathy	Personal learning goals, in and out of school Success criteria Emotions in success Making a difference in the world Motivation Recognising achievements Compliments	Taking personal responsibility How substances affect the body Exploitation including 'county lines' and gang culture Emotional and mental health Managing stress	Mental health Identifying mental health worries and sources of support Love and loss Managing feelings Power and control Assertiveness Technology safety Take responsibility with technology use	Self-image Body-image Puberty and feelings Conception to birth Reflections about change Physical attraction Respect and consent Boyfriends/girlfriends Sexting Transition

3. The Role of Technology in our Pupils' Lives

Current and emerging technologies used in and outside of School include: websites, email and instant messaging, blogs, social networking sites, chat rooms, music/video downloads, live streaming, video sharing, gaming sites, virtual reality and augmented reality devices and games, text messaging and picture messaging, video calls, podcasting, online communities via games consoles and mobile internet devices such as smart phones, tablets and smartwatches.

This communication revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Ibstock Place School to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation. They also need to learn how to prevent the risks and report any concerns that may occur.

4. Responsibilities: Technical Staff

Filtering, monitoring and blocking technologies are used in School.

The technical staff, Network Manager and Executive Director of Innovation & Strategic Programmes have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of our hardware system and our data on the network (although all staff with

access to data are responsible for its security). They monitor the use of the internet and emails and will report inappropriate usage to the Management Team.

5. Responsibilities: Designated Safeguarding Lead (DSL)

We recognise that internet safety is a child protection issue, so the DSL, the Co-Heads of Prep and Class Teachers, take a lead role in all aspects of internet safety training for staff, pupils and parents.

The School's comprehensive PSCHE and Computing curriculum on E-Safety is the Co-Heads', DSL, Subject Lead for Computing and Subject Lead for PSCHE's responsibility. They will ensure that all pupils in the School are educated in the risks and the reasons why they need to behave responsibly online. It is their responsibility to handle allegations of misuse of the internet and to discuss such instances with the Co-Heads and Head.

The Co-Heads of the Prep School host a Digital Parenting Evening each year for parents in Kindergarten to Year 6 when important changes are applicable to the school. The Subject Lead for Computing provides resources for EYFS, Key Stage 1 and Key Stage 2 in order to help facilitate 'E-Safety' Weeks, 'Safer Internet Day' and specific lessons addressing how to stay safe online and with technology.

There is additional advice for pupils and parents of Prep 6 on the Wellbeing Hub.

6. Responsibilities: Teaching Staff

Ibstock Place School ensures that staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology both in and out of School, e.g., use of passwords, logging off, use of content, research skills and copyright. Teachers of Computing ensure pupils only use School-approved systems and publish within appropriately secure/age-appropriate environments.

Information and Communication Technology has transformed the entire process of teaching and learning at Ibstock Place School. It is a crucial component of every academic subject and is also taught as a subject in its own right. All classrooms are equipped with computers, iPads, interactive screens and, in some cases, projectors, for use by teachers.

Pupils have access to either desktop computers, laptop computers or iPads. The Prep School has a Computing Suite with 24 computers, 48 iPads and class iPads are also available. The pupils

are taught in a spiral curriculum, alternating between using iPads, desktop computers, and learning about staying safe online.

Pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different sites and why some apparently authoritative sites need to be treated with caution.

In the Prep Schools, online research is supervised by teachers. The filtering and monitoring system of Senso is used throughout the Prep and Senior School, and any concerns are sent immediately to the IT department, Network Manager and DSL.

In the Early Years Setting, the School insists that:

- Personal mobile phones should be either turned off or on silent and not accessed during working hours.
- Mobile phones can only be used during a designated break, and this must be away from the children.
- Mobile phones should always be stored safely in designated areas during working hours. The Head of Pre-Prep has a designated lock box for safe storage of devices.
- During outings, staff should only use mobile phones in an emergency.
- Photographs must not be taken of the children on any personal phones or any other personal information storage device. Only School-owned devices can be used to take photographs or videos.
- Staff must not use personal mobile phones to communicate with parents/carers unless it is an emergency.
- Staff who bring personal mobile phones into the provision must ensure that there is no inappropriate or illegal content on them.
- The early years setting is not responsible for the loss, damage or theft of any personal mobile device.
- All members of staff should remain vigilant and report any concerns to the setting's manager or designated safeguarding lead (DSL). Parents and staff should be informed of the complaints procedure, and staff should be made aware of the whistleblowing procedure.
- If a member of staff is thought to have illegal content on a mobile phone or has committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed.

For pupils, Smart watches/devices are not allowed in School. This is because they are a distraction and may interrupt learning. Smart-free mobile phones are only allowed to be brought in by pupils in Year 6 and some extenuating circumstances, e.g. spending time in separate households after School. These are handed in during morning registration and

returned to the pupils at the end of the day. The phones should not be used until pupils are off the school site.

7. Prep 6 Pupils

It is important that any parents allowing a smart-free phone to be brought into School are fully aware of how they will be looked after and the sanctions that will be imposed in the event of misuse.

- Smart-free phones are to be switched off.
- Smart-free phones are to be handed into the Class Teacher and locked away at the beginning of the day. They will be returned at the end of the day in class.
- It cannot be guaranteed that these cupboards will be locked at all times, as members of staff require access to resources/materials/possessions.
- The taking of photographs and video footage using a camera phone is strictly prohibited.
- Any children found to have taken photographs/videos will be asked to delete the photos in the presence of a member of the Primary Leadership Team.
- If it is suspected that a child has not handed in their phone or if a device is audible in a bag, members of Staff may look in the pupils' possessions to assist with the situation. The device will always be kept safe and handed back at the end of the day.
- Rules about devices on School trips (including residential trips) and sports fixtures remain the same. Pupils are not allowed to use their phones, should hand them in to the teacher in charge and will be given them back at the end of the day. Parents should be contacted if this is deliberately disobeyed.

Misuse: Statement of Policy

The Prep School will not tolerate any illegal material. If we discover that a child or young person is at risk as a consequence of online activity, the parents will be contacted in the first instance. This will also be logged on the safeguarding system of My Concern.

A range of sanctions may be handed out to any pupil who misuses technology to bully, harass or abuse another pupil in line with our *Anti-Bullying, Anti-Cyber Bullying and Behaviour Policy*.

8. Passwords

All staff and pupils are told to keep their passwords and PINs private. If a password is compromised, the School should be notified immediately. Passwords are generated at the beginning of the year, and the master copy is kept by the IT Department, Computing Lead and Co-Heads. Pupils may change their passwords, but should there be a problem, it may be reset by the IT Department.

9. Staff Training

Staff attend CPD and additional training sessions with the Subject Lead for Computing, Subject Lead for PSCHE and external educational specialists in order to teach new skills, highlight important new legislation and guidance and also to input additional resources to help when teaching pupils how to stay safe online.

10. Involvement with Parents

The Prep School seeks to work closely with parents and guardians in promoting a culture of E-Safety. The Co-Heads or DSL will always contact parents if there are any worries about their child's behaviour in this area and hope that they will feel able to share any worries with the School.

The Prep School encourages an open conversation in which pupil safety is the priority and they must feel safe in reporting incidents online, whether this be by them or to them. Peer-on-peer abuse online will never be tolerated, and sanctions will be decided in line with the *Anti-Bullying and Anti-Cyber Bullying* and *Behavioural Policy.* Parents will be informed immediately if there is an incident involving their child, either being abused or abusing online.

The Prep School recognises that not all parents may feel equipped to protect their child when they use electronic equipment at home. There are opportunities for parents to learn about the potential hazards of technology and understand how practical steps can be taken to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. We encourage an open conversation at home as well.

11. School Closure

In order to ensure that e-safety measures were put in place during the national lockdowns, an additional policy was created. See the *'Remote Learning Policy'* for specific details.

Queries

Queries on this policy should be directed to the Prep School Co-Heads and DSL.

Review and Verification

This policy is reviewed annually by the Primary Management Team members delegated as responsible for e-safety.

Appendices

Please see overleaf.

Appendices

IBSTOCK PLACE SCHOOL

CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." Dr Tanya Byron, "Safer Children in a digital world: the report of the Byron Review".

E-safety is a whole School responsibility, and at Ibstock Place School, the staff and pupils have adopted the following charter for the safe use of the internet inside the School:

Cyberbullying

- Cyberbullying is a pernicious form of bullying and our School's *Anti-Bullying and Anti-Cyberbullying Policy* describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at School, but everyone needs to learn how to stay safe outside the School.

Treating Other Users with Respect

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the School Rules [copies of which are sent to parents and are in the Pupil Planner].
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School is committed to promoting equal opportunities for all, regardless of faith, race, gender, gender orientation, sexuality or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or a worrying issue, to a member of the pastoral staff.

Keeping the School Network Safe

- We adhere to the BECTA guidelines regarding E-teaching and the internet.
- Certain sites are blocked by our filtering system and our IT Department monitors pupils' use of the network.
- The IT Department monitors email traffic and blocks SPAM and certain attachments.
- We issue all pupils with their own personal School email address. Access is via personal LOGIN, which is password-protected. We give guidance on the reasons for always logging off and for keeping all passwords secure.
- Access to sites such as "Hotmail" is not allowed on the School's network.
- We have strong anti-virus protection on our network, which is operated by the IT Department.
- Any member of staff or pupil who wishes to connect a removable device to the School's network is asked to arrange in advance with the IT Department to check it for viruses.

Promoting Safe Use of Technology

Pupils of all ages and parents are encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International (www.childnet.com)
- https://www.bbc.co.uk/newsround/44074704
- Staying Safe – Own It – BBC
- Online Safety for Children – Tips & Guides | NSPCC
- Digizen (www.digizen.org)
- Chat room dangers (www.chatdanger.com)
- Child Exploitation and Online Protection(www.ceop.police.uk and www.thinkuknow.co.uk)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

They prepare their own models of good practice, which may form the subject of presentations at Assemblies. They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft.

Safe Use of Personal Electronic Equipment

- Our guidance is that caution should be exercised before putting personal information on the web.
- We offer guidance on the safe use of social networking sites and cyberbullying in Tutorial Day lessons, which cover blocking and removing contacts from "friend lists".
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- We give guidance on how to keep safe at home, by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content. Similarly, IPS covers how a mobile phone filter can be activated and how to block nuisance callers.

IBSTOCK PLACE SCHOOL

Acceptable Use Agreement (Prep School)   [Form]

NAME: Forename Surname

School Username: Forename Surname

School Email Address: ForenameSurname@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 ICT equipment at School.

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.

- I will use School computers for Schoolwork and not to upset or be rude to other people.

- I will only use my School email account (which ends in @ibstockplaceSchool.co.uk) in School.

- I will not open any email attachments without checking with an adult.

- I will only go on websites and search engines that my teacher tells me to.

- I will tell my teacher straight away if I go on a website by mistake.

- I will tell a teacher straight away if I see a website I did not try to open, or receive emails from people I don't know.

- I will look after School ICT equipment and tell a teacher straight away if something is broken or not working properly.

- I will not try to download or install any software on School computers.

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

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

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

I understand that all of my work and internet activity on School ICT 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 ICT equipment at School may be stopped, my parents and teachers will discuss what I have done wrong and there may be further punishment.

Child's Signature: ....

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

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

ICT Use Pupil Agreement (Senior School)

Email, Internet and Network Policy

Introduction

We want each pupil 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. The computers 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 good behaviour 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 which 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 equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) either by wire or wirelessly without the prior permission of the Network Manager.
- Do not eat or drink near computer equipment.
- Do not use the School network for creating any materials which are unlawful, obscene or abusive.

Security and Privacy

- You must change your password from '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 discipline.
- Never tell anyone you meet on the Internet your home address, your telephone number, your School's name, or send them your picture, unless you are given permission to do so.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- 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 review files, Internet use and email communications to ensure that users are using the system responsibly.

Internet and Email

- Do not access the Internet or use email unless for study, or for School authorised/supervised activities.
- 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. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem to be.
- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- You must not bring the School into disrepute through your use of email or the Internet.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or Schools is strictly forbidden. This applies to any material of violent, dangerous, racist, or

inappropriate content. Always report such messages to a member of staff.
- Do not, at any time (including during ICT Club), use the School network to play non-educational games.

Pupils may not have access to the School's Email, Internet and Network facilities unless this signed contract is returned to the Network Manager. 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.

CONTRACT

When you have returned this contract, 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.

NAME: «PUPIL-txtfullname»   YEAR GROUP: «PUPIL-intenrolmentncyear»

Please note that your username is: «pupil-txtforename»«pupil-txtsurname»

(one word, no spaces or punctuation)

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

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

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

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

ICT Use Staff Agreement

Email, Internet and Network Policy

Title Forename Surname

Introduction

The School has provided ICT facilities for the use of staff 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 of the School's ICT facilities.

Equipment – do not:

- Install, attempt to install, or store programs of any type on the computers without the agreement of the Network Manager.
- Attempt to disassemble any equipment – refer problems to the ICT Help Desk.
- Use the computers for commercial purposes, e.g. buying or selling goods.
- Open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) or via email until they have been checked with antivirus software, and have been found to be clean of viruses.
- Connect or attempt to connect any equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) either by wire or wirelessly without the agreement of the Network Manager.
- Eat or drink near ICT equipment.
- Use the School network for creating any materials which are unlawful, obscene or abusive.

Security and Privacy:

You must change your password from 'pa55word' 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. If a computer is logged on by another person and you wish to use it, but you cannot find that person, please log that person off before proceeding. If in doubt, please contact the Network Manager or ICT Technician.
- 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 employment conditions.

- Access to the data on the School network is provided to you solely for the execution of your professional duties and belongs to the School and may not in any form or on any media be used, distributed or in any way passed to another party for any reason whatsoever.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Tell a member of the ICT staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else, so that a note may be made if required against the log.
- For your own protection and that of others, files, Internet use and email communications may be reviewed to ensure that users are using the system responsibly.

Internet and Email:

- The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn.
- The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with work commitments. Personal use is a privilege and not a right. If the School discovers that you have breached these requirements, disciplinary action may be taken.
- You must not bring the School into disrepute through your use of email or the Internet.
- Never open attachments to email messages unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- Sending or receiving email containing material likely to be unsuitable for children or Schools is strictly forbidden. This applies to any material of violent, dangerous, racist, or inappropriate content. Always report such messages to a member of the ICT staff.
- Information in the Staff Handbook about the nature of correspondence and the procedure for checking it must be observed.

Staff may not have access to the School's email, Internet and network facilities unless this signed contract is returned to the Network Manager. The School regularly monitors the use of the internet and email systems to check that the use is in accordance with this

policy. If it is discovered that any of the systems are being abused or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your access to the network being 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.

Your Details

Name: Forename Surname

User Name: InitialSurname

Email address: InitialSurname @ibstockplaceSchool.co.uk

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

Signature of staff member: