Policy 5.10

Acceptable Use of Technology Policy

Updated:	01.09.26
Reviewed by:	DP
Next Review date:	01.09.27

Kitebrook Preparatory School Policy 5.10 Acceptable use of Technology Policy

1. **It is the responsibility of the Designated Safeguarding Lead, together with the Director of IT to review and update this policy annually.**

2. **Scope of this Policy**

2.1 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 IT systems. In addition, this policy covers the use of personal digital devices accessing 3G and/or 4G while on school premises. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes all carers and guardians of pupils. 'Visitors' include occasional volunteers and all other ad-hoc visitors.

2.2 The term 'digital device' in this policy includes Chromebooks, mobile phones, iPads, tablets, laptops, smart watches, MP3, MP4 players, e-readers and any internet enabled device.

3. **Introduction**

3.1 It is the duty of Kitebrook Preparatory School [hereafter 'the School'] to ensure that every pupil in its care is safe; the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

3.2 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:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles;
- Mobile internet devices such as smart phones and tablets.

3.2 Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

3.3 At Kitebrook, we understand 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. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

4. Roles and Responsibilities

4.1 The Head and the Senior Leadership Team
The Head is responsible for the safety of the members of the school community including their e-safety. The Head has delegated day-to-day responsibility for e-safety to the Designated Safeguarding Lead (DSL) who is supported by the Heads of Sections.

4.2 In particular, it is the role of the Head and Senior Leadership Team (SLT) to ensure that:

4.3 All staff, and in particular the Designated Safeguarding Lead, is trained about e-safety as part of the wider safeguarding training, 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.

4.4 Designated Safeguarding Lead
The Designated Safeguarding Lead is accountable to the Head for all day to day issues relating to e-safety and has responsibility for ensuring that this policy is upheld by all members of the school community, and is required to work with IT staff to achieve this. Safeguarding training and online safety training go hand in hand.

4.5 Supported by the E-Safety Officer and other subject matter experts drawn from across the School, the DSL will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the Independent Schools Inspectorate, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Child Partnership.

4.6 IT Support
The Director of IT ensures the School's technical staff have a key role in maintaining a safe technical infrastructure, training all school staff that have access to the School's IT systems, monitoring data traffic which includes filtering, and keeping abreast of the rapid succession of technical developments. Additionally, the IT Dept will generate inappropriate usage reports to the DSL as required.

4.7 Staff
All members of the School community who have a school network login are required to sign the Acceptable Use Policy (Appendix 1). Mobile phones are not permitted to be used in pupil areas.

4.8 EYFS
Personal mobile phones and other personal devices with the capability to take photographs (e.g smart watches) are not permitted in the EYFS or when teaching EYFS pupils.

4.9 As with all issues of safety at Kitebrook, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

4.10 Pupils
Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy (Appendix 1). They must inform staff if they see IT systems or digital devices being misused.

4.11 Parents and carers
The School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. The School will provide opportunities to consult and discuss e-safety with parents and will seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if there are any concerns about a pupil's behaviour in this area and it is expected that parents will feel able to share any concerns with the school.

4.12 Parents and carers are responsible for understanding and helping enforce the school's E-Safety policy.

5. Policy Statements

5.1 Use of School and Personal devices
Staff- School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them, for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

5.2 Staff are permitted to bring in personal devices for their own use but may not use such devices, phones and tablets for teaching. Devices may be used to receive school email. No non-school provided device should be used on the school's network without the permission of the Director of IT first. Staff must not plug anything into the school's network.

5.3 Personal telephone numbers, email addresses, or other contact details should not be shared with pupils or parents / carers. Where possible, Staff should avoid contacting a pupil or parent/carer using a personal telephone number, email address, social media, or other messaging system.

5.4 Pupils - those in Years 4 - 8 have their own Chromebook that has been configured to use at school. The School has other Chromebooks available for pupil use. Access to these devices is only available when approved by a member of staff.

5.6 The School recognises that digital devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a digital device for such purposes, the pupil's parents or carers should arrange a meeting with the Head or DSL to agree how the school can appropriately support such use. They will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

6. Use of internet and email

6.1 Staff must not access social networking sites, online shopping or any website or personal email which is unconnected with school work or business from school devices, whilst teaching or in the presence of pupils. Such access may only be made from staff members' own devices away from pupils. School email addresses must not be used to subscribe to services that are not connected to school work/business

6.2 When accessed from staff members' own devices, staff must use social networking sites with extreme 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.

6.3 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.

6.4 Staff must immediately report to the Director of IT or if unavailable, the DSL or Head, 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.

6.5 Any online communications by staff must neither knowingly or recklessly:

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

6.6 Under no circumstances should pupils be added as social network 'friends' or contacted through personal social media accounts. Each member of staff is responsible for ensuring high privacy settings across their personal social media accounts.

6.7 Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Staff should not contact a pupil or parent / carer using any personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business. Staff are made aware that email communications through the school network and school email addresses are monitored as they are the property of the School.

6.8 Volunteers are permitted access to emails; however wider access to IT systems will be restricted.

6.9 All pupils are issued with their own personal school email address for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service, Gmail, along with other products in the Google Workspace, is regarded as safe and secure, and must be used for accessing all school work, assignments / research / projects. Pupils are made aware that email communications through the school network and school email addresses are monitored as they are the property of the school.

6.10 There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the Director of IT for assistance.

6.11 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 Director of IT or if unavailable, the DSL or Head.

6.12 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.

6.13 Pupils must report any accidental access to materials of a violent or sexual nature directly to the Director of IT or if unavailable, the DSL or Head or another member of staff. Deliberate access to any

inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with in accordance with the "Rewards and Sanctions Policy". Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

7. Data storage and processing

7.1 The School takes its compliance with the UK General Data Protection Regulation (the "UK GDPR") and the Data Protection Act ("DPA") 2018 seriously.

7.2 Please refer to the school's Privacy Policy and the Acceptable Use Policy for further details.

7.3 Staff and pupils are expected to save all data relating to their work to the school's Google Drive systems.

7.4 Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on portable storage devices, such as memory sticks.

7.5 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of IT or if unavailable, the DSL or Head.

8. Password security

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

8.2 All pupils and members of staff must:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which will be changed every 90 days;
- not write passwords down;
- not share passwords with other pupils or staff.
- never give the school's WIFI password out to anyone

9. Safe use of digital and video images

9.1 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.

9.2 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 networking sites).

9.3 Parents/carers may not take videos and digital images of their children at school events or on school property, unless expressly permitted to do so in accordance with the Photographs Policy. To respect everyone's privacy and in some cases protection, any images taken should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission

of their parents or carers), nor should parents or carers comment on any activities involving other pupils in the digital/video images.

9.4 Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Photographs Policy concerning the sharing, distribution and publication of those images. Those images should, where possible, be taken on school equipment. If personal equipment is used, this should first be discussed with the DSL for permission; any images taken should be uploaded straight away onto the school network and deleted immediately from the personal device.

9.5 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.

9.6 Pupils may only take, use, share, publish or distribute images of others if it is in line with the Photographs Policy.

9.7 Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see Parent Contract/Acceptable Use Policy for more information). The School Office will ensure staff are aware of whose photos may not be used.

9.8 Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

10. Misuse

10.1 The 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 the Oxfordshire Safeguarding Children Partnership (Local Safeguarding Children Partnership). If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP (Child Exploitation and Online Protection).

10.2 Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy).

10.3 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 Policy.

11. Complaints and Concerns

11.1 As with all issues of safety at Kitebrook, if a member of staff, a pupil or a parent / carer has a complaint or concern, they should refer to the Complaints Policy for further information.

11.2 Incidents of or concerns around e-safety will be recorded using CPOMS (online pastoral logging system) and the Designated Safeguarding Lead will act in accordance with the school's Child Protection Policy.

12. Education and Training

12.1 Staff: Awareness and Training

- All new staff will receive information on the school's Safeguarding, E-Safety, including Acceptable Use and Digital Device policies as part of their induction and will be required to sign to confirm that they accept and understand the procedures therein.
- All staff are to receive information and training on e-safety issues in the form of INSET training and internal meeting time. They are to be made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff must also receive information about e-safety as part of their safeguarding induction on arrival at school.
- 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 Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are following the school's IT guidelines.
- Teaching staff are encouraged to incorporate e-safety and awareness-raising activities 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 DSL and Head on CPOMS.

13. Pupils: e-Safety in the curriculum

13.1 IT and online resources are used increasingly across the curriculum. The School believes it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

13.2 The School provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via RHC lessons, through presentations in assemblies, as well as informally when opportunities arise.

13.3 Pupils are taught about their e-safety responsibilities and to look after their own online safety. In a graduated and age appropriate manner, the pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at the School.
In a graduated and age appropriate manner, the pupils are taught laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

13.4 Pupils should be 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 Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach any member of staff as well as parents and peers for advice or help if they experience problems when using the internet and related technologies.

14. Parents

14.1 The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

14.2 The School recognises that not all parents and guardians may feel equipped to protect their children when they use digital devices at home. The School therefore provides information for parents about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

14.3 Pupils' own Chromebooks have been configured to always have the Schools' filtering system, Securly, in place and work, even when the device is used outside of school

Appendix 1

Acceptable Use of IT and the Internet

for Pupils and Staff Policy

This policy is the responsibility of the Designated Safeguarding Lead together with the Director of IT to review and update annually.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, carers, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers.

Kitebrook Preparatory School and the Internet

The computer network is owned by Kitebrook and is made available to pupils to further their education and to Staff to facilitate their roles. It is to support and enhance learning and teaching as well as for carrying out the business of the School. Access to the Internet is provided through a filtered education provider for the safety of all users.

All members of the Kitebrook community must sign an Acceptable Use of IT and the Internet Agreement when they join Kitebrook and thereafter at the start of every academic year.

Appendix 2

Acceptable Use of IT and the Internet Agreement for Pupils in Years 3 – 8

Any pupil wishing to use the Kitebrook Network and Internet access must agree to follow this Acceptable Use Policy. By signing this document, you are giving the School permission to monitor your usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails, and to search and monitor any emails or Internet sites visited. Pupils requesting Kitebrook Network and Internet access should sign this copy of the Acceptable Use Policy and return it to The School Office.

Pupils must only use their own account. Login details must not be shared with others. This will be dealt with as an equally serious offence as using another person's account.

Parents / Guardians are requested to endorse their child's signature.

As a School user of the Internet, I agree to follow the School rules on its use.

- I will abide by the School Code of Conduct and the Digital Device policy regarding the use of internet enabled devices, such as Chromebooks.

- I will use the network in a responsible way and observe all the restrictions explained to me by the School.

- I give express consent for the monitoring and searching of my School account (my emails, internet usage and documents). My personal digital devices can be searched by a senior member of staff in my presence.

- I understand that breaking any of these rules may lead to suspension of my access to the Internet or computer network (or both). I also understand that misuse of technology, both inside and outside School, which affects the welfare of members of the School community or the reputation of the School will be subject to disciplinary procedures.

- I understand that the school owns the computer network and can set rules for its use. I understand it is a criminal offence to use a digital device or network for a purpose not permitted by the school.

- I will not do, write or publish anything using my personal digital device, such as a smart phone and iPads, that I would not be prepared to show to my parents, or carers, the Head or a future employer.

- I will choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships.

- I will not be obscene either in the words I use or the content I view. This includes material that is racist, violent or adult in nature.

- I will not store or access inappropriate or illegal material.

- I will not send or post electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
- I will respect the laws of copyright and ensure that sources used are referenced.

- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details.

- I will not take or distribute any images, video or audio recordings of any staff or pupils without their consent.

- I will not upload or distribute electronically any image, video or audio content relating to the School or a Staff Member of the school community without permission from the Head

- I will never use my device to bully, physically threaten or upset anyone and will report any instances of bullying that I know about.

- I will report all instances of bullying on social media affecting any pupils at Kitebrook and I will recognise, even if I am not directly responsible for it, I have a duty to report it.

- I understand that inappropriate use of the internet (including during holidays) may lead to disciplinary action according to the Rewards and Sanctions policy.

- I will use my digital device as directed by my teachers and will do nothing to bring the school into disrepute.

- I will not send anonymous messages or chain mail.

- I will not attempt to circumvent the schools filtering in any way.

- I will not access or attempt to access unauthorised areas of the school network or any other computer network. This includes logging on to another user's account.

- Torrenting, peer-to-peer networks or illegal file sharing are not permitted.

- I will acknowledge and adhere to the E-Safety rules

- I understand that the school can check my computer files, emails and monitor the internet sites I visit.

Name of pupil: _____

Signature:_____ Date:_____

As the parent / guardian of the above-named pupil, I grant permission for my child to use electronic mail and the Internet in School. I understand that my child will be held accountable for their own actions.

Name of Parent / Guardian:_____

Parent/Guardian's signature:_____ Date:_____

Appendix 3

Acceptable Use of IT and the Internet Agreement for Pupils in EYFS and Years 1 & 2

Any pupil wishing to use the Kitebrook Network and Internet access must agree to follow this Acceptable Use Policy.

By signing this document, you are giving the School permission to monitor your child's usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails, and to search and monitor any emails or Internet sites visited.

To ensure that all pupils understand the requirements of the Acceptable Use Policy regular time is allocated to the teaching of e-safety, including a dedicated lesson at the beginning of every term. In an age appropriate manner, all pupils are taught how to follow the Acceptable User Rules. They are reminded of the importance of keeping themselves safe on the Internet; how to follow the Internet Safety Rules; how to behave on the Internet and what to do when asked for personal information. Pupils are also made aware that should they choose to break the Acceptable Use rules they will be subject to age appropriate disciplinary procedures.

Parents / Guardians are requested to sign the Acceptable Use Policy on behalf of their child.

Child's Full Name:_____

Year Group:_____

Your child will be expected to adhere to the following:

*I will use the network in a responsible way and observe all the restrictions explained to me by the School.

*I give express consent for the monitoring and searching of my School account (my emails, internet usage and documents). My internet-enabled and/or communication devices can be searched by a senior member of staff in my presence.

*I understand that breaking any of these rules may lead to stopping access to the Internet or computer network (or both). I also understand that misuse of technology, both inside and outside School, which affects the welfare of members of the School community or the reputation of the School will be subject to disciplinary procedures.

As the parent / guardian of the above-named pupil, I grant permission for my child to use electronic mail and the Internet in School. I understand that my child will be held accountable for their own actions.

Name of Parent / Guardian:_____

Parent / Guardian's signature:_____

Date: _____

Appendix 4

Acceptable Use of IT and the Internet Agreement for Staff

Any member of staff wishing to use the Kitebrook network and internet access must agree to follow this Acceptable Use Policy. By signing this document, you are giving the School permission to monitor your usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails and to search and monitor any emails or Internet sites visited. Staff requesting Kitebrook network and internet access should sign this copy of the Acceptable Use Policy and return it to the Director of IT.

Staff must access the computer network only via their own account and password, which must not be available to any other person. Passwords should be strong and all users will be prompted to change these regularly.

Staff are responsible for the content of the emails they send. Emails must be formal and appropriate. Emails and messages sent to other forums accessed via the School network are School property and will be monitored. Posting anonymous messages and forwarding chain letters is forbidden.

If any pupil or member of staff is personally insulted, abused, libelled or bullied through the Internet or School network, this must immediately be reported to the Head. Any abuse of the Internet or electronic device technology inside or outside School, which has a significant impact on School life, will also come under this policy.

All activities that threaten the integrity of the School IT systems or attack or corrupt other systems are forbidden. These include hacking, deliberate spreading of viruses, manipulating and deleting files other than their own and creating macros to the same end. Staff must respect the copyright of materials found on the internet.

Staff must also respect the right of others to privacy and confidentiality.

Staff must not (both during and following the termination of their employment) when using the internet or any social networking site:

- post or publish any derogatory reference to the School, colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene or libellous;
- discuss pupils or colleagues negatively or criticise the School or its staff; or
- misuse or inappropriately alter any text (written or audio), images or video clips featuring members of the School community.

Staff must also respect the right of others to privacy and confidentiality. Text, images or clips of the School or members of the School staff can only be uploaded on School accounts on official School business in an appropriate manner and for no other purpose. Text, images or clips of pupils must not be uploaded to any internet site or distributed electronically without permission from the individual or their parent. This applies to both the School network and personal network. Please refer to the Photographic Images policy.

Staff must not attempt to avoid the filtering system in any way to gain access to restricted internet sites. Staff must never use any network to access or spread inappropriate materials such as radicalising, pornographic, racist, sexually harassing or offensive text and images. They must never use School access to the Internet to pursue personal gain including online auctions, gambling, own political purposes/activism or advertising. Staff must immediately report to the Director of IT or if

unavailable, the DSL or Head if they encounter undesirable material during any kind of communication on the internet or computer network. Staff must not store inappropriate or illegal material.

The Acceptable Use Policy also applies to staff who use their own laptops or any other internet-enabled device. All devices must be password protected as a minimum and where possible encrypted. In addition, all laptops must have anti-virus software. It is the responsibility of each member of staff to keep this up to date and to ensure that all updates are installed. Laptops without anti-virus software will not be configured to access the network or Internet.

Misuse of technology, both inside and outside of school, which affects the welfare of members of the school community or the reputation of the school will be subject to disciplinary procedures.

Staff must be aware that their access to all files and emails sent or received on school systems will be suspended and the contents may be deleted following the end of their employment. It is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague.

As a School user of the Internet, I agree to follow the School rules on its use:

- I will use the network in a responsible way and observe all the restrictions explained to me above

- I give express consent for the monitoring and searching of my School account (my emails, internet usage and documents).

- I understand that breaking any rules in the policy may lead to removal of my access to the internet or computer network (or both). I also understand that any misuse of technology by me, either inside and outside of School, which affects the welfare of members of the School community or the reputation of the School will be subject to disciplinary procedures.

Staff Full Name:_____

Department:_____

Staff Signature:_____

Date:_____