Court Fields School

Online Safety Policy

Guidance Policy for IT Acceptable Use

Template January 2025

Approved by the Local Governing Committee:

Next review date: January 2027

Introduction

IT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to guide and teach in use of these technologies in order to arm our young people with the skills to access the benefits of the technology safely, and know how to implement and interact with further technologies as they emerge.

IT covers a wide range of resources including, web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of IT within our society as a whole. Currently the online technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Social Media
- Video Sharing and Streaming Services
- Music Downloading and Streaming
- Gaming
- Smartphones and devices with messaging, video and internet connectivity

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly across Social Media platforms and other online services, is not consistently policed. All users need to be aware of the range of risks associated with the use of these online technologies.

At Court Fields School we understand the responsibility to educate our pupils about Online Safety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our schools to use technology to benefit learners.

Everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This policy is inclusive of devices provided by the school and those owned by pupils and staff but used to access School IT services.

Monitoring

IT Support staff authorised by the School Business Manager, the Headteacher or their designated deputy, Blackdown Education Partnership Trust IT Manager or Head of IT, may inspect any IT equipment owned or leased by the School or Trust at any time without prior notice. IT staff may also monitor, intercept, access, inspect, record

and disclose telephone calls, emails, instant messaging, internet use and any other electronic communications involving its employees or contractors, without consent, to the extent permitted by law. This may be as part of their normal working practices; be to confirm or obtain School or Trust business related information; to confirm or investigate compliance with School or Trust policies, as part of a disciplinary investigation; to ensure the effective operation of School or Trust IT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation 2018 and/or Data Protection Act 2018; to prevent or detect crime.

IT authorised staff may, without prior notice, access the email or any data stored on the School or Trust's IT systems, or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the General Data Protection Regulation 2018, Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School or Trust IT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All activity on School/Trust owned devices, and all access and activity within Trust systems, is logged by the Trust. These logs may be monitored by authorised IT Staff, who are required to report concerns to the Designated Safeguarding Lead. Certain keywords are flagged which may result in a screen shot being saved and reported directly to DSLs or other Safeguarding Staff as determined by the Headteacher or SLT.

Policy Breaches

Any policy breach may be grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Data Breach Reporting

Any, data breaches or unauthorised access, IT must be immediately reported to the your School's Data Protection Lead, or Data Protection Officer – along with notifying IT Support and/or the Trust IT Manager. Additionally, all loss or theft of equipment, suspected misuse of IT, or virus/malware notifications, IT should be reported to the IT Helpdesk.

All other policy non-compliance must be reported to your School Business Manager or Trust IT Manager.

Suspicious emails should be reported to the IT Support Team via the Report Email functionality with the Outlook Microsoft365 system. Simply right click on the email in the list, choose Report, then Phishing. This will submit the email to Trust IT Support and to Microsoft for review in a safe and secure manner. Do NOT forward suspicious emails to the IT Helpdesk or any other person.

Online Safety

Roles and responsibilities

As Online Safety is an important aspect of strategic leadership within the School, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. To support in this work a member of the School's Senior Leadership Team has been designated as the Online Safety Co-ordinator for the school – the named Online SafetyCo-ordinator is Sarah Westwood It is the role of the Online Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, NCSC, DfE, CEOP (Child Exploitation and Online Protection), Childnet & UK Safer Internet Centre.

The Senior Leadership Team and governors are updated by the Headteacher / Online Safety Co-ordinator so they have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This purpose of this policy, supported by the School's acceptable use agreements for pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory policies: safeguarding and child protection, health and safety, and behaviour (including the anti-bullying) and PSHE.

Online Safety in the curriculum

IT and online resources are used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

- The school has a framework for teaching internet skills in IT and PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about Online Safety
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum
- Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by

  any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, (i.e. parent/carer, teacher/trusted staff member, or an organization such as Childline or CEOP)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the IT curriculum Pupils are provided age-appropriate lessons on what AI is, how it works, and its potential benefits and risks. This foundational knowledge helps pupils make informed decisions when using AI tools.

Online Safety skills development for staff

- Our staff receive regular information and training on Online Safety and Cyber Security issues in the form of annual briefings and NCSC training.

- New staff receive information on this Online Safety Policy as part of their induction and are asked to confirm that they have read and will follow it at all times
- All staff have been made aware of individual responsibilities relating to the safeguarding of children and the KCSIE guidance within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community
- All teaching staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas

Email

The use of email within schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.

Staff and governors are all provided with their own email account to use for all school business as a work based tool. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The School email account should be the account that is used for all School business

Staff and governors

- Under no circumstances should staff or governors contact pupils or parents with regard to any school business using personal email addresses
- Emails created or received by staff or governors as part of their School role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000, or a Subject Access Request under General Data Protection Regulation 2018 and/or Data Protection Act 2018 . Staff must therefore actively manage their email account as follows:
    - Delete all emails of short-term value
    - Organize email into folders and carry out frequent house-keeping on all folders and archives
- Staff and governors must inform the Designated Safeguarding Lead and their line manager if they receive an offensive email from a school stakeholder.

Pupils

- Pupils may only use school approved accounts on the school system.
- All pupil email users must ensure that they do not use inappropriate language and do not reveal any personal details about themselves or others in email communication.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive email
- Pupils are introduced to email as part of the IT Scheme of Work

Sending emails

Staff and governors should follow the following guidelines:

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section entitled - 'Emailing Personal, Sensitive, Confidential or Classified Information'
- Keep the number and relevance of email recipients, particularly those being copied in, to the minimum necessary and appropriate.
- When sending emails to external organizations, parents or pupils, check the email carefully before sending, in the same way as a letter written on school headed paper. The email must include the sender's name and job title. Email content should always be polite and tolerant of the views of others and will reflect the standards expected of an employee of Blackdown Education Partnership.
- Do not send or forward attachments unnecessarily.
- If sending to a group of unacquainted external recipients, ensure that addresses are added to the Bcc field to ensure recipients cannot see each other's addresses, which could constitute a Data Breach.
- School email is not to be used for personal advertising except with the express permission of the Headteacher.

Receiving emails

Staff, governors and directors should follow the following guidelines:

- Check their email regularly including their junk email box as legitimate emails (particularly from parents using webmail accounts) may end up there
- Activate their 'out-of-office' notification when away for more than 2 working days.
- Never open attachments from an untrusted source; Report the email as laid out in the Section entitled "Data Breach Reporting" or consult the IT Support Team first. Do NOT forward the email to any other person to do this.
- Automatic external forwarding of emails is not allowed unless authorized by IT Support.

Emailing Personal, Sensitive, Confidential or Classified Information

If confidential information has to be emailed externally, the following guidelines should be followed:

- Do not send the information to any person / organisation whose details staff have been unable to separately verify (usually by phone).
- If emailing to an external recipient, then it should be sent using the encryption tools within Microsoft365, or if necessary, as an encrypted attachment.
- If encrypted attachments are used, provide the encryption key or password by a separate email or ideally an alternative contact for the recipient(s).
- Request confirmation of safe receipt.
- Do not identify such information in the subject line of any email.
- Do not put a pupil's name or initials in the subject line but mark it as CONFIDENTIAL

Pupils with additional needs

The School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the School's Online Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Internet access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged. Systems are in place to detect and flag inappropriate use. This may be acted on immediately upon detection, and/or if concerns are raised.

Use of the Internet

- Staff must preview any recommended sites before use
- Any on-line educational resources which require uploading student details must have prior approval of the School's Data Protection Lead (DPL).
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material. The School's filtering systems will endeavour to stop all inappropriate sites wherever possible, but this must not be considered 100% reliable as sites are constantly being changed, added, and updated – sometimes maliciously.
- In the event that inappropriate material is accidentally accessed it must be reported to a member of the IT Support team immediately
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe software copyright at all times. It is illegal to copy or distribute School / Trust software or software from other sources
- All users must observe copyright of materials from electronic resources including multimedia resources such as YouTube.

Infastructure

- Court Fields School and Blackdown Education Partnership are aware of their responsibilities when monitoring staff communication under current legislation and takes into account; General Data Protection Regulation 2018, Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school-based email and internet activity is monitored and can be accessed if required

- The School uses management and control tools for controlling and monitoring workstations and logging user activity, including web browsing. This extends to all School devices whether in school or elsewhere.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the IT Support Team or Teacher as appropriate
- Pupils and staff are not permitted to download programs onto School-based technologies without seeking prior permission from the IT Support Team.
- If there are any issues related to viruses or anti-virus software, the IT Support Team should be informed immediately.

Protecting Against Cyber Threats: Phishing, Malware, and Ransomware

In today's digital age, it's crucial to be aware of cyber threats and take proactive steps to protect yourself. Here are some key strategies to safeguard against phishing, malware, and ransomware

Phishing Protection:

- Be Sceptical: Always be cautious of unsolicited emails, messages, or phone calls asking for personal information. Verify the sender's identity before responding
- Check URLs: Hover over links to see the actual URL before clicking. Look for misspellings or unusual domain names.
- Avoid Sharing Sensitive Information: Never share personal or financial information through email or text messages. Legitimate organizations will not ask for such details this way.
- Use Multi-Factor Authentication (MFA): Enable MFA on your accounts to add an extra layer of security on all 3rd party accounts, if available. MFA is enforced on all Staff login accounts, when accessing School and Trust IT Systems from outside of the School sites.

Ransomware Protection:

- Be Cautious with Email Attachments: Do not open email attachments from unknown or suspicious sources, or even from a known source if it was not expected. Even familiar sources can be compromised.
- Educate Yourself: Stay informed about the latest ransomware threats and how they spread. Awareness is key to prevention.
- By following these guidelines, you can significantly reduce the risk of falling victim to cyber threats and keep your information and devices secure. Stay vigilant and proactive in your online activities!

Suspicious emails should be reported to the IT Support Team via the Report Email functionality with the Outlook Microsoft365 system. Simply right click on the email in the list, choose Report, then Phishing. This will submit the email to Trust IT Support and to Microsoft for review in a safe and secure manner. Do NOT forward suspicious emails to the IT Helpdesk or any other person.

If you are concerned you may have already open, clicked or submitted to a malicious email, or you have a virus or malware alert, please report that immediately to the IT Helpdesk. The sooner it is reported, the more chance there is of containing it.

Student Use of Social Media

The Internet, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Definitions and Scope

Social networking applications include, but are not limited to: Online discussion forums, Collaborative spaces, Media sharing services, and online gaming environments. Examples include X(formerly Twitter), Facebook, YouTube, Xbox Live, Instagram, Snapchat, TikTok etc.

At present, the school endeavours to deny access to social networking sites to pupils within school

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, email address, social media names, specific hobbies/interests)
- Our pupils are advised to set and maintain profiles on such sites to only show their name and profile picture publicly, and to deny access to any unknown individuals

Our pupils are asked to report any incidents of online bullying to the school

Staff and Governor Use of Social Media

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our School, the Trust, the community, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The purpose of this section of the Online Safety Policy is to:

- Safeguard all children.
- Protect the School and Trust from legal risks.
- Ensure that the reputation of the School, the Trust, its staff and governors are protected.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

All staff and governors should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and this policy.

Within this policy there is a distinction between use of school sanctioned social media for professional educational purposes, and personal use of social media.

Personal use of social media

- School employees and governors must not do anything to risk the safeguarding of pupils or to harm the reputation of the School or Trust in any posts, comments or communications on any social media platform
- Any concerns regarding any communication received from children must be reported to the School's Designated Safeguarding Lead.
- If any member of staff, governor or director is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Staff and governors should not routinely accept current students as 'friends' except in exceptional circumstances (e.g. close family friends etc.)
- All privacy settings must be set to ensure that no personal information, other than that intended, is shared on personal social media accounts.
- Staff and governors are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- This policy must be adhered to at all times including on School trips and when absent from school due to illness etc.
- Staff and governors will ensure that any online activity outside the School will not bring the School or Trust into disrepute

School sanctioned use of social media

There are many legitimate uses of social media within the curriculum and to support student learning.
When using social media for school purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- No such social media accounts should be setup, without the express consent of the Headteacher, Marketing Officer, or other authorised role.
- The URL and identity of the site should be notified to the appropriate Head of Department or member of the SLT before access is permitted for students
- The content of any school sanctioned social media site should be solely professional and should reflect well on the school.
- Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published
- Care must be taken that any links to external sites from the account are appropriate and safe

- Any inappropriate comments on or abuse of school sanctioned social media should immediately be removed and reported to a member of SLT
- Staff should not engage with any direct messaging of students through social media where the message is not public

Sexting

Sharing photos and videos online is part of daily life for many young people, enabling them to share their experiences, connect with friends and record their lives. Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps, such as Instagram, Snapchat, WhatsApp, TikTok, or Facebook Messenger. This increase in the speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is also illegal. This includes imagery of yourself if you are under 18. Although the production of such imagery is most likely to take place outside of school and college, these issues often manifest in school.

The National Police Chiefs Council (NPCC) made clear in 2016 that "incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues". The NPCC also stated that "Schools should respond to incidents without involving the police provided that the young person shared the imagery consensually and there is no intended malice. Any such cases should be dealt with by the school directly". They went on to say however that incidents should be referred to the Police if there were aggravating factors such as a young person sharing imagery "without consent and with malicious intent".

When an incident involving youth produced sexual imagery comes to the school's attention:

- The incident should be referred to the Designated Safeguarding Lead (DSL) as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved, if appropriate
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person. In most cases the imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms.

- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment

- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents will be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- You have reason to believe any pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then the school may decide to respond to the incident without involving the police or children's social care. The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework.

Searching devices, viewing and deleting imagery

Viewing the imagery

Adults should **never** view youth produced sexual imagery unless there is good and clear reason to do so. The decision to view imagery should be based on the professional judgement of the DSL and should always comply with the safeguarding policy and procedures of the school. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil. If a decision is made to view imagery the DSL would need to be satisfied that viewing is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved).

If it is necessary to view the imagery then the DSL should:

- Never copy, print or share the imagery; this is illegal.
- Discuss the decision with the Headteacher.
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Headteacher.
- Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- Ensure viewing takes place on school premises, ideally in the office of the Headteacher or a member of the senior leadership team.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery.
- Record the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions
- Ensure this is signed and dated.

If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a young person or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school

systems) then the DSL should ensure that the staff member is provided with appropriate support. Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

Deletion of images

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery.

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone has been seized, a senior member of staff who has been formally authorised by the Headteacher can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.

In most cases young people should be asked to delete imagery and to confirm that they have deleted the imagery. In normal circumstances adults should not search through devices and delete imagery unless there is good and clear reason to do so. Young people should be reminded that possession of youth produced sexual imagery is illegal. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the young person. At this point the school may want to invoke their own disciplinary measures to discourage young people from sharing, creating or receiving images but this is at the discretion of the school in line with its own behaviour policies.

Recording incidents

All incidents relating to youth produced sexual imagery must to be recorded either in a safeguarding chronology or in the Behaviour module of the School's Management Information System, or other specialised Safeguarding software, whichever is most appropriate. This includes incidents that have been referred to external agencies and those that have not.

Teaching young people about sexual imagery

We recognise that teaching about safeguarding issues in the classroom can prevent harm by providing young people with skills, attributes and knowledge to help them navigate risks. Learning about youth produced sexual imagery cannot be taught in isolation. Learning about youth produced sexual imagery will be taught through the PSHE programme, as well as in the school's IT programme of study where it will reflect the requirements of the National Curriculum programme of study for computing. Given the potential sensitivity of these lessons it is essential that this issue is taught within an emotionally safe classroom climate where clear ground rules have been negotiated and established and where boundaries around teacher confidentiality have been clarified. If during any lesson teachers suspect any child or young person is vulnerable or at risk the school's safeguarding protocols should always be followed.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and also to be aware of their responsibilities.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement:
    - "Ensure my child understands and signs the School's IT Acceptable Use Agreement"
- The school disseminates information to parents relating to Online Safety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website/Learning Platform posting
    - Newsletter items
    - Learning platform training

Passwords and Password Security

Passwords

Staff and governors should follow the following guidelines:

- Do use anyone else's logon details to access IT-based services.
- Change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Never disclose your password to anyone else, with the exception of IT Support Staff who may, in rare circumstances, request it to provide troubleshooting. This situation will always be avoided if at all possible.
- Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- User ID and passwords for staff, governors, and pupils who have left the School are removed from the system as soon as possible.

If any staff member of governor think their password may have been compromised, or someone else has become aware of their password, they must change it immediately and report it to the IT support team.

Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and

not to share with others, including their friends. Staff and pupils are regularly reminded of the need for password security.

- Users are provided with an individual IT Systems username.
- Pupils are not allowed to access on-line materials or files on the Trust IT Systems which belong to their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the Trust IT Systems. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic lock time for the school network is 10 minutes

  If ever using a Shared Device to login to the Trust IT Services, you must ensure all systems are fully logged out when finished.

Safe Use of Images

Taking of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the School permits the appropriate taking of images by staff and pupils with School
- Staff are not normally permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken using these devices provided they are transferred immediately and solely to the secure storage facilities provided via the School's IT Systems and deleted from the staff device and any storage media.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others without their express consent, this includes when on field trips.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Pupils' Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site.
- on the school's Learning Platform.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/transmitted on a video or webcam.
- in display material and on electronic displays that may be used in the schools' communal areas.
- in display material that may be used in external areas, i.e. exhibition promoting the school.

- general media appearances, (e.g. local/national media/press releases sent to the press highlighting an activity whether sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue, (e.g. divorce of parents, custody issues, etc.)

Parents/carers may withdraw permission, in writing, at any time.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the members of Staff authorised by the Senior Leadership Team or BEP Head of IT have authority to update the website.

Storage of Images

- Images/films of children are stored on the Trust's secure storage facilities.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher. If these are used they must be encrypted.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the Trust IT Systems.

Webcams and CCTV

- Schools within the Blackdown Education Partnership use CCTV for security and safety. A separate CCTV policy governs this area.
- We do not use publicly accessible webcams in school.

School IT Equipment including Portable & Mobile IT Equipment & Removable Media

School IT Equipment

- As a user of IT, staff are responsible for any activity undertaken on the School's IT equipment provided to them.
- The School will log IT equipment issued to staff and record serial numbers as part of the School's inventory.
- Visitors, Staff and Pupils are not allowed to plug IT hardware into the School network points (unless expressly authorised by IT Support). Visitors should be directed to the wireless connectivity facilities if available.
- Staff should ensure that all IT equipment that they use is kept physically secure.
- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material)
- It is imperative that staff save their data on a frequent basis to the School's storage system where it will be securely backed up. Staff are responsible for the backup and restoration of any of their data that is not held on the School's storage system.

- User data should not be stored on the local drives of PCs. If it is necessary to do so, and this must be authorised by IT Support, the local drive must be encrypted and backups must be made
- Staff must not display sensitive data on a classroom display screen (TV or projector)
- Privately owned IT equipment should not be used on the School's network without prior approval of the IT Support team. They may use any BYOD Wi-Fi provision (where available), without approval.
- The School's IT system must not be used for any non-School business or commercial purposes
- On termination of employment, resignation or transfer, staff must return all IT equipment to their Manager.
- It is a staff member's responsibility to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant IT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA). This must be done via the IT Support Team.

Portable & Mobile IT Equipment

This section covers such items as laptops, and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material).
- Staff must ensure that all data is stored on the secure storage facilities provided by the School's IT systems and that the device is synchronised to these systems on a frequent basis
- Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- No other person or user should use or have access to your user account on any devices.
- Ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades, or IT maintenance requirements
- The installation of any applications or software packages must be authorised by the IT support team, fully licensed and only carried out by IT support
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied
- Portable equipment must not be used to record meetings unless agreed by all parties present

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as smartphones, tablets, laptops, gaming devices, and etc are familiar to children outside of school. They often provide a collaborative, well-known device with internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our schools choose to manage the use of these devices in the following ways so that users exploit them appropriately.

Staff use of School Mobile Devices (including phones)

- Staff are responsible for the security of their school mobile phone. They should always set the PIN code on their school mobile phone and must not leave it unattended and on display (especially in vehicles).
- Staff must report the loss or theft of any school mobile phone equipment immediately.
- The staff member will be responsible for all call costs made on a stolen phone until the phone is reported lost or stolen.
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material)
- Staff must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it.
- School SIM cards must only be used in school provided mobile phones without prior approval from IT Support
- Staff must not send text messages to premium rate services.
- When overseas, data roaming should be turned off and only switched on for brief periods if no Wi-Fi is available – unless prior arrangements for roaming data packages have been made and approved.

Staff use of Personal Mobile Devices (including phones)

- The School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/carer using their personal device.
- The School (or Trust) is not responsible for the loss, damage or theft of any personal mobile device
- Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device
- The sending of inappropriate communications between any member of the School community is not allowed
- Mobile phones must not be used to record meetings unless agreed by all parties present

Pupil use of Personal Mobile Devices (including phones)

- Pupils are allowed to bring personal mobile devices/phones to school but only if they are switched off at all times within the school day and are in their bags or coats.

- This technology may be used, however for educational purposes under the express permission of the class teacher. The device user, in this instance, must always ask the prior permission of the bill payer
- Mobile phones cannot be used at break or lunchtime.
- The School (or Trust) is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate communications between any member of the School community is not allowed
- Permission must be sought before any photos, video or sound recordings are made on these devices of any member of the School community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Mobile phones must not be used to record meetings unless agreed by all parties present

Removable Media

- Due to the accessibility of the secure storage facilities provided via the Trust's IT Systems there should be no requirement to store any school data on removable media.
- If circumstances do require the use of removable media, there must be no sensitive or confidential information stored on it, unless the media is encrypted.
- Users must be aware that data on removable media is not backed up and any data loss will likely be irreversible.

Review Procedure

There will be an on-going opportunity for staff to discuss with the Online Safety Coordinator any issue of Online Safety that concerns them.

There will be an on-going opportunity for staff to discuss with either the IT Support Team or the Designated Safeguarding Lead any issue of data security that concerns them.

This policy will be reviewed every 2 years and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Current Legislation

Acts relating to monitoring of staff email

General Data Protection Regulation 2018
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to Online Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

General Data Protection Regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Appendix 1

Acceptable Use of the School's IT System and the Internet (by Students)

The school's IT system (inc. access to the Internet, email and other digital resources) are there to support your learning. To help keep you safe and everyone else safe and to ensure that you make use of these resources in a way that is appropriate and legal the following rules have been put in place. Please read them carefully and if there is anything you don't understand, please ask your tutor or IT teacher.

I agree that:

- I will never share my password with anyone or use anyone else's password. If I become aware that my own password has become known to someone else, or I find out someone's password I will immediately inform the IT Support Team
- I will never infringe the security or privacy of another user. I will never attempt to access or alter their files or folders, or tamper with their storage area on the school system or any removable media (e.g. USB drive) they may have.
- I will do everything I can to keep myself and others safe on the Internet. I will never disclose or publicise personal information about myself or others (e.g. home address or telephone / mobile number), nor will I respond to requests to meet with someone that I do not know.
- I will always treat others with respect and will never harass, threaten, harm, insult or offend them.
- During lessons, I will only use the school's IT systems and equipment for educational purposes linked to the learning objectives of the lesson. At break and lunchtimes I may use the facilities for personal purposes provided they meet the other sections of the policy
- I will take care of all IT equipment and the IT environment and I will not remove any IT equipment from its current location, either temporarily or permanently.
- I will not download or bring into school unauthorised programs, or attempt to install or store them on the school's IT system or on any of its equipment.
- I will never knowingly introduce a virus or other malware to the school's systems
- I will not access or download inappropriate (e.g. pornographic, racist or offensive) materials and will ensure that none of my files contains such material. This includes viewing, displaying, downloading, and printing, sending, or otherwise transmitting materials.
- I will switch off or close my screen immediately and report to a teacher if I discover an unsuitable site.
- I will not access social media websites, or messaging services (inc chat sites) using the school's system. I will not access online games sites during lessons

- I am aware of the ‘Report It’ button and know when to use it.
- I will not take photos, or make audio or video recordings of another student or member of staff without their permission.
- I will never send or forward inappropriate images of myself (or others) to another person and understand that to do so is criminal offence.
- I will not copy information into assignments without fully acknowledging the source of it. I understand that if I break this rule it could be classed as plagiarism and/or copyright infringement and so have serious consequences, particularly where the work is being submitted for exam purposes.
- I will not submit, or attempt to submit, content created using Artificial Intelligence (AI) as my own work.
- I will not copy or distribute any copyrighted material (inc software, video, music etc) and understand that it is illegal to do so.
- I will only use my school email account for school work and school related activities. When writing, or replying to emails I will always be polite towards others and tolerant of their views in what I say. The same applies to any attachments I may send.
- I will only open emails (and any attachments) if they come from someone I already know and trust.
- I will not send spam or spoof emails or emails containing hoax virus warnings.
- I understand staff may review my files and communications (inc. emails) where there are concerns about the content and/or to ensure that the system, equipment and other media are being used responsibly. This may include random checks.

Please remember that if you act in an inappropriate manner your access rights may be withdrawn, which would adversely affect your learning, and further sanctions may also be imposed.

Acceptance of the above conditions:

Full Name: _____Tutor Group: _____

Signature: _____Date: _____

Parent’s Signature: _____ Date: _____