CASTLE COURT
SCHOOL

e-Safety Policy

including Technical Security Policy

Reviewed October 2025

Due for Review October 2026

B Cheadle (E-Safety champion) & P Dunsford (DSL)

Development / Monitoring / Review of this Policy

This policy relates to all departments within the school including our EYFS nursery department. It has been created using the latest version of the SWGfL template and has been developed by e-Safety Coordinator and Network manager with consultation through a range of informal meetings having completed the SWGfL Audit. The school uses an e-Safety Group to undertake in part the Development / Monitoring / Review of this policy.

e-Safety Group **(click to link to general description of roles and** *terms of reference*)

- *Child Protection – designated safeguarding lead: Mr Paul Dunsford (who takes overall responsibility for e-Safety in the school)*
- *Head of e-learning, e-Safety champion and Network Manager: Mr Ben Cheadle*
- *Child Protection / Safeguarding Governor with responsibility for e-Safety: Mrs Hannah Doust*
- *Section Leaders: Ms Kirsty Thompson, Mrs Louise Munns, Mr Andy Laidler, Mr Graham Antell*
- *Parent representative: Mrs Long*
- *Pupil representative: Thor Long & Alexandra Hill*

Castle Court School will monitor the impact of the policy using:

- *Logs of reported incidents – presented to governors at the Termly Educational Committee Meetings*
- *Monitoring logs of internet activity using Smoothwall and Securus Software*
- *Feedback from the e-Safety group meetings*

Scope of the Policy

This policy applies to all members of Castle Court School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Castle Court School.

The Education and Inspections Act 2006 empower Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off Castle Court School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this policy, which may take place outside of Castle Court School, but is linked to membership of Castle Court School.

The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data (please refer to CCS Searching, Confiscation, Deleting and Safe-Storage Policy). In the case of both acts, action can only be taken over issues covered by the published Child Protection Policy and Behaviour, Discipline and Exclusion Policy.

Castle Court School will deal with such incidents within this policy and associated behaviour and anti-bullying policies (please refer to CCS Anti-Bullying Policy) and will, where known, inform parents / carers of incidents of inappropriate e-Safety behaviour that take place out of school.

An effective Online Safety Policy must be tailored to the needs of each school, and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. It is best practice that the school reviews their Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new technological developments or trends in technology related behaviours.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to ***online safety*** *empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*

"Governing bodies and proprietors should ensure ***online safety*** *is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how* ***online safety*** *is reflected as required in all relevant policies and considering online safety*

whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"

The DfE Keeping Children Safe in Education guidance also recommends:
Reviewing online safety *… Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.*

The DfE Keeping Children Safe in Education guidance suggests that:

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
content: *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*
contact: *being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*
conduct: *online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*
commerce: *risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 require schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

Roles and Responsibilities
The following section outlines the e-Safety roles and responsibilities of individuals and groups within Castle Court School:

Governors
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee (education) receiving regular information about e-Safety incidents and monitoring reports. Mrs Hannah Doust of the Governing Body has taken on the role of e-Safety Governor which has been combined with that of the Child Protection / Safeguarding Governor. The role of the E-Safety Governor will be to meet with the e-Safety Co-ordinator to discuss the e-Safety policy and how it is being applied.

Head and Senior Leaders
The Head has a duty of care for ensuring the safety (including e-Safety) of members of the Castle Court community, though the day-to-day responsibility for e-Safety will be delegated to the e-Safety Co-ordinator (the DSL) and e-Safety champion.
The Head should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff. **"Responding to incidents of misuse"**

Designated Safeguarding Lead and e-Safety Co-ordinator - Mr Paul Dunsford
The DSL is trained in e-Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials (including production/sending of youth produced sexual imagery)
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- They therefore take overall responsibility for e-Safety in the school

NB: it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

As part of this the DSL will: -

- take day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing Castle Court School e-Safety Policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments
- meet annually with the e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend the relevant Governors Sub Committee (education) meeting
- report e-Safety incidents to Senior Leadership Team

Dealing with e-Safety incidents will follow the guidelines laid out in the Castle Court Behaviour, Discipline and Exclusion Policy. Investigations, actions, and sanctions will depend on the level of incident and will involve one or more members of staff, ranging from the Head teacher, Assistant Head (Pastoral), Class/form teacher and e-Safety Co-ordinator.

In their role as Designated Safeguarding Lead, the e-Safety Co-ordinator has a particular brief to ensure that the correct procedures are followed if/when a pupil may be at increased risk of significant harm due to risks associated with e-Safety: in such instance he will follow the Child Protection Policy and Procedures.

e-Safety Champion – Mr Ben Cheadle

CCS acknowledges the need to have a named member of staff to assist the e-Safety Co-ordinator. The e-Safety champion will: -

- lead the e-Safety group
- help to monitor, embed, and review Castle Court School e-Safety procedures and policies
- help to deliver e-Safety training to Parents, Staff, Governors, and children, including annual e-Safety Day, liaising with the Assistant Head-Pastoral/DSL over ongoing training requirements for pupils
- to complete the annual SWGfL 360 e-Safety audit and present the findings to the e-Safety group
- report to the DSL on any incidents relating to Child Protection issues
- report to the Governors' Education Committee on a termly basis

Network Manager – Mr Ben Cheadle

Castle Court School has managed ICT services provided by outside contractors. It is the responsibility of Castle Court School to ensure that the Network Manager together with the managed service providers carry out all the e-Safety measures that would otherwise be the sole responsibility of Castle Court School technical staff. Mr B Cheadle is responsible, in conjunction with the managed services Castle Court School subscribes to (SWGfL, Smoothwall, Securus, RM, Police Data Collection, Ripple) for ensuring:

- that Castle Court School's technical infrastructure is secure and is not open to misuse or malicious attack
- that Castle Court School meets required e-Safety technical requirements as set out by this policy and SWGfL e-Safety Guidance
- that users may only access the networks and devices in a secure manner
- the filtering policy (which forms part of the Technical Security Policy) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety technical information to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / internet/ remote access / email is regularly monitored in order that any misuse / attempted misuse will be reported to the e-Safety Coordinator or Assistant Head-Pastoral, for investigation depending on the case
- that monitoring software / systems are implemented and updated as mentioned in the Technical Security Policy section

Dorset Police Contact -

Hannah Bird - cyberchoicesdorset@dorset.pnn.police.uk

Teaching and Support Staff

The teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of e-Safety matters and of the current CCS e-Safety Policy
- they have read, understood the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the e-Safety Coordinator or Head teacher / Assistant Head-Pastoral, for investigation depending on the case
- all digital communications with pupils / parents / carers should be carried out using official school systems
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-Safety and Responsible Use Policy and pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies & devices in lessons and other school activities and implement current policies regarding these devices (Photographic, Audio and Video)
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*.
- they adhere to the school's technical security policy, regarding the use of devices, systems and passwords and understand basic cybersecurity.
- they have a general understanding of how the learners in their care use digital technologies out of school, to be aware of online safety issues that may develop from the use of those technologies.
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit.

There is an expectation that professional standards will be applied to online safety as in other aspects of school life

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence.
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff can reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes.
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
- *Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.*

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from Castle Court School community, with responsibility for issues regarding E-Safety and monitoring the E-Safety Policy including the impact of initiatives. The E-Safety Coordinator will also be responsible for regular reporting of the group to the Governors Sub Committee (education).

Members of the e-Safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of Castle Court School e-Safety Policy / documents
- the production / review / monitoring of Castle Court School Filtering Policy which forms part of the Technical Security Policy, and requests for filtering changes
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth, and progression within the CAVE (Character and Values Education) and Computer syllabus
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils

All pupils at Castle Court School:

- are responsible for using Castle Court School digital technology systems in accordance with the **Responsible Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that Castle Court School*'s* e-Safety Policy covers their actions out of school, if related to their membership of Castle Court School
- should know how to report an incident – older pupils can use the CEOP link in RM unify to file a report
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly with Artificial Intelligence services

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Castle Court School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, and information about national/ local e-Safety campaigns / literature. Parents and carers will be encouraged to follow guidelines on the appropriate use of

- digital and video images taken at school events (please see Photographic, Audio and Video recording of children section**)**
- Use of mobile phones in and around school and school trips and sports fixture

Community Users (including parents, visitors, event organisers and participants)

Community Users who access school systems / website / Guest Wireless Network as part of the wider school provision will be expected to accept the Guest User Acceptable Use policy before being provided with access to

school systems. Where a third party is providing a service to the school and is given access to school databases or sensitive information, they will sign a third-party data sharing agreement. (See Appendix 2).

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of Castle Court School's e-Safety provision. Children and young people need the help and support of Castle Court School to recognise and avoid e-Safety risks and build their resilience.

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-Safety curriculum should be provided as part of CAVE (Character and Values Education)/ Computing lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Responsible Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – parents / carers

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Castle Court School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, e-Safety guides
- High profile events / campaigns e.g., Safer Internet Day
- Social media videos/posts created by our Year 8 leaders
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

In the longer term it is proposed that Castle Court School could provide opportunities for local community groups / members of the community to gain from Castle Court School's e-Safety knowledge and experience. This could be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy, and e-Safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents
- Castle Court School website could provide e-Safety information for the wider community
- Supporting community groups e.g. Early Years Settings, childminders, youth / sports / voluntary groups to enhance their e-Safety provision

Education & Training – Staff / Volunteers
It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly
- It is expected that some staff will identify e-Safety as a training need within the performance management process
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand Castle Court School e-Safety policy and Acceptable Use Policy
- The e-Safety Coordinator will receive regular updates through attendance at external training events (e.g., from SWGfL and other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / department meetings / INSET days
- The e-Safety Coordinator / will provide advice / guidance / training to individuals as required
- **the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff**

Training – Governors
Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e-Safety / health and safety / child protection. This may be offered in several ways:

- Attendance at training provided by the Local Authority / National Governors Association / or another relevant organisation (e.g., SWGfL)
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies)
- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Technical – infrastructure / equipment, filtering, and monitoring
Castle Court School together with the managed ICT service providers will be responsible for ensuring that Castle Court School infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

Please click here for a more detailed in Technical Security Policy. (which includes Filtering Policy)

- School technical systems will be managed in ways that ensure that Castle Court School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school's technical systems. The Smooth Wall boxes are updated whenever a new patch is released. Each month, the Network Manager checks and updates any server patches that are required. He also receives a newsletter from the Cyber Police Data Collector. Securus Logs are checked on a weekly basis and the Network Manager also 'pushes out' the latest windows update patches to all new devices each week during term time. When Smooth Wall or Securus breaches arise, these are logged.
- Servers, wireless systems, and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices
- All KS2 users will be provided with a username and secure password, EYFS & KS 1 will be supplied with unique username but a generic password by the IT Department who will keep an up-to-date record of users and their usernames
- Users are responsible for the security of their username and password
- The "master / administrator" passwords for Castle Court School ICT system, used by the Network Manager are also held by the Head of ICT. They must, however, also be available to the Head and kept in the school safe
- The account passwords for YouTube, Instagram, Mums-net, Twitter, CCS Website, eBay.... used by CCS Marketing and Admin are also held by the Network Manager & Head of ICT. They must, however, also be available to the Head and kept in the school safe
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband and filtering provider by actively employing the Internet Watch Foundation CAIC list.
- There is a clear process in place to deal with requests for filtering changes (please refer to Filtering section within the in Technical Security Policy. section). Castle Court School has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on Castle Court School technical systems and users are made aware of this in the Responsible / Acceptable Use Policy Agreements. (CCS uses SWGfL, Smoothwall, Ripple and Securus. for the monitoring programmes that are used)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of Castle Court School systems and data. These are tested regularly. Castle Court School infrastructure and individual workstations are protected by up-to-date virus software
- A Guest User Acceptable Use policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, inspectors, visitors) onto Castle Court School systems
- An agreement is in place regarding the extent of personal use that staff users and their family members are allowed on school devices that may be used out of school. (Please refer to Staff Acceptable Use Policy
- Pupil and Staff users are not allowed to use any form of removable media. Please refer to the CCS Data Protection Policy regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on school devices
- Personal data cannot be sent over the internet or taken off Castle Court School site unless safely encrypted or otherwise secured. Please refer to the CCS Data Protection Policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying 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. Castle Court School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites,

nor should parents / carers comment on any activities involving other pupils in the digital / video images

- Staff who have signed the schools' Photography / Videography declaration' have permission to take digital images/ videos to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images.
- 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 Castle Court School into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or 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.
- Permission from parents or carers will be obtained before photographs of pupils are published on Castle Court School website (may be covered as part of the Annual Data Collection signed by parents or carers at the start of the year –
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Photographic, Audio and Video recording of children
Privacy

- No person is authorised to take images of children that:
- might cause embarrassment or distress; or
- are associated with distressing or sensitive issues; or
- are unnecessarily intrusive.

If there is any doubt about these matters, the person wishing to take the image must obtain the written consent of the child's parent(s). Filming and photography by television or newspaper journalists will take place only with the consent of the Head and under appropriate supervision. When images are taken for publication by television or newspaper journalists, children will only be named if there is a reason to do so (for example if they have won a prize) and home addresses will not be given out.

Promotional material

It is an implied term of the contract for educational services which exists between the school and the parents of a pupil, that photographs of the pupil may be taken and used by the school in accordance with normal custom and practice. Such custom and practice will include set piece photographs of the school, form, team, theatre cast and snapshots of School activities.

It has also been custom and practice for independent schools to use images of their pupils for marketing purposes, such as in prospectuses and promotional videos or displays on its website. Parents who do not want their child's photograph or image to appear in any of the school's promotional material must make sure that their child knows this and must write immediately to the Head, requesting an acknowledgement of their letter. Such permission is also sought through the Annual Data Collection Sheets which are sent out to parents soon after the start of the academic year.

Taking of images by parents and friends

Parents and friends often wish to take images of their children at school plays and concerts or sporting activities. Courtesy and good manners require that the following rules are respected:

- if visitors ask whether they can take photographs, they should be reminded that whilst it is permissible under the Data Protection Act 1998 to take photographs for personal use, publication of such images may be unlawful: this includes, but is not limited to, the uploading of such material onto the internet

However, as a concession, images that feature the child of the parent who has taken the images may be uploaded to the internet, provided that no other children or staff members are identifiable from the images: if such people are identifiable in the images, their permission (or, in the case of a child, that of their parent(s)) must be sought before uploading to the internet; this includes any images taken at school events, whether they include a child or not; where a play or concert or other event is subject to copyright and performing rights restrictions, visitors will

not be permitted to take images, photographs or video film. In many cases, official photographs or videos may be available for sale, however.

Publishing of images on the school website and approved social media sites (See Social Media Policy)

Photographs from school events are made available to parents. However, Parents must adhere to the measures explained within this document. (Taking of images by parents and friends)

Early Years Foundation Stage (EYFS)

Within the EYFS, the use of mobile phones and smart watches with photo-imaging technology and/or video capacity is strictly forbidden, by parents, visitors, and members of staff other than those using a school mobile device (MDM), following the consent of the Head of EYFS. This means that their use for any purposes is not permitted within the Badger and Reception Classrooms and the Badger play area. When pupils from EYFS are using facilities in the wider school (for example, the adventure playground, the outer playground, and the woods), the use of mobile phones and/or smart watches is strictly forbidden.

Colleagues from other departments are not to use mobile phones and/or smart watches when passing through or alongside the EYFS department. The guiding principle is that no EYFS pupils should ever see a mobile phone (other than a school phone) while at school. This extends not only to members of staff but also to parents and visitors in the school. As a result, visitors may be asked to put their mobile phone away in and around the EYFS department. Signage has been put up in the EYFS department to draw this to the attention of visitors.

Seeking consent

Although consent of parent(s) or pupils is not always a legal requirement, the school will seek express prior written consent:

- for use of portrait style images of pupils
- for use of pupils' images by or with commercial sponsors

Photographs and other images taken by members of staff for the purpose of their professional role within the school (e.g., for self-portraits in art, for sport technique coaching, as part of an academic lesson) may be taken and used within the school without additional parental consent. However, at all points colleagues should ensure that their use of such images is beyond reproach. The dissemination of such images beyond the Castle Court community, without appropriate consent being gained, would be viewed as a serious disciplinary offence.

As part of the school's ongoing commitment to child protection, colleagues are not permitted to make use of their own photographic equipment without having first signed a 'staff photography / videography declaration' which outlines the increased responsibilities required of colleagues in such circumstances. Any colleagues with questions about such usage should contact the DSL in the first instance. In the updated DfE guidance on mobile phone usage in schools (2024), it states that 'there may be occasions where it is appropriate for a teacher to use a mobile phone to issue rewards and sanctions (P8). At Castle Court, members of our sports and CAVE (Character and Values Education) teams, who are regularly working 'outside the classroom' are required to do this to utilise our whole school behaviour management app, Track it Lights.

Care needs to be taken on match days and other events at which Castle Court pupils are playing against or working alongside pupils from other schools. As a courtesy, colleagues in such a situation should seek permission from the member of staff with responsibility for the children from the other school. This permission should never be presumed.

Photographs as part of pupil records

Passport-style photographs form part of the pupil's personal record. These images are subject to the Data Protection Act 1998 and will therefore:

- be stored securely
- not be used for any other purpose without the consent of the pupil or his or her parent(s)
- not be shown, copied, or given to any unauthorised person

Use of camera enabled devices by pupils in school

Those pupils who have permission to make use of mobile devices are reminded that permission does not extend to using camera/video capabilities. All pupils must allow staff access to images stored on (mobile phones and/or) cameras and must delete images if requested to do so. Images taken by pupils under these arrangements may not be uploaded to the internet by the child without the permission of any identifiable pupils or members of staff

featured in them but may be uploaded by the relevant member of staff for educational purposes, providing permissions have been sought where appropriate (see 'Seeking Consent' above).

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. Contravention of these rules constitutes a serious breach of school discipline and pupils doing so can expect to be disciplined accordingly. All pupils and parents are directed towards the school's Behaviour, Discipline and Exclusion policy.

Child protection (see Child Protection Policy)

Staff will be mindful of child protection issues and will raise concerns with the DSL if they become aware of anyone:

- taking an unusually large number of images
- taking images in inappropriate settings such as cloakrooms, toilets or changing areas
- taking images of children who are apparently unaware that they are being photographed or filmed

Audio Recordings

In some cases, there may be a need for teachers within their professional responsibilities to make recording of pupils' voices (for example, in music and MFL lessons). The use of such recordings is limited to the confines of the school, and they should not be disseminated further than the school, except for the purposes of external assessments (for example, a French aural or a recording of a performance piece ahead of an assessment for a music scholarship). Additional permissions will not be sought from parents for such recordings.

Rule

We are particularly mindful of the multi-functionality of many hand-held devices currently on the market – including but not exclusive to; smartwatches, cameras, mobile phones, e-readers, and video cameras, particularly those with internet capabilities (3G/4G/5G). While there may be opportunities to use school owned equipment of this nature as part of a bona fide school project, all such devices are not to be brought into school or used on the school minibuses to/from school.

Enforcement

Pupils breaking this rule can expect to be dealt with in line with the school's published Behaviour, Discipline and Exclusion policy. The device should be confiscated by the member of staff who is made aware of it and deposited with the Head's Secretary for safe keeping. Parents will then be contacted, an evening detention administered, and parents will then be required to collect the device from the Head's secretary (her office hours are 0900-1615 Monday to Friday).

School Trips

The only exception to this rule is the use of mobile phones, smartwatches, e-readers, mp3 players or games consoles on school trips. Where a journey is more than 1 hour long (i.e., not regular games fixtures or a 'local' visit) or the duration of the trip is more than 24 hours (i.e., overnight), the Group Leader of such a trip may decide – in consultation with the Educational Visits Co-ordinator and members of the Senior Management Team – to allow some (but not necessarily all) types of handheld device. In those circumstances when devices with internet capabilities are permitted, this will only take place with a full briefing for parents and pupils on their usage and an appropriately worded code of conduct, signed by both pupils and parent(s). Such trips will be viewed on a case-by-case basis and parents will be fully informed prior to the trip of any allowance that is being made for such usage during the trip. Pupils must not assume that such devices are permitted on a trip merely because it involves a long journey or is overnight: they should seek clarification from the Group Leader of the trip.

The Group Leader should make a written log of all such devices on the trip. As with all such valuables, any equipment brought to school or taken on a trip under this exception will be at the parents' risk and the school encourages parents to ensure that property is both clearly named and insured.

Mobile Phones

All staff should follow the guidance given in the Code of Conduct Policy with regards to use of Mobile Phones and Social Contact and the Staff Photography / Videography Declaration (see Appendix 3 at the end of this document)

Data Protection
(please see separate CCS Data Protection Policy)

Communications
The following table shows how Castle Court School currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies & Removable Media	Staff & other adults				Pupils			
	Allowed at certain times	Allowed for selected staff	Allowed	Not Allowed	Allowed at certain times	Allowed for selected pupil	Allowed	Not Allowed
Encrypted Removable Media (Memory Sticks, Flash Cards)				X				X
Non Encrypted Removable Media (Memory Sticks, Flash Cards, CD/DVDs)				X				X
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons	X							X
Use of mobile phones in social time	X							X
Taking photos on mobile phones / cameras		X						X
Use of other mobile devices e.g., tablets	X							X
Use of personal email addresses in school or school network		X						X
Use of school email for personal emails				X				X
Use of messaging apps		X						X
Use of social media	X							X
Use of blogs	X							X

**Visiting Staff can give a piece of Removable Media to the Network Technician so that the information can be added to the school's network.*

When using communication technologies Castle Court School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only Castle Court School email service to communicate with others when in school, or on school systems (e.g., by remote access)

- Users must immediately report, to an appropriate adult/colleague, any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. An appropriate adult/colleague depends on the severity of the incident but includes: The Head, Assistant Head-Pastoral, Head of E-learning, Classroom Teacher
- Any digital communication between staff and pupils or parents / carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- All pupils from Rec (EYFS), KS1, KS2 and above will be provided with individual school email addresses for educational use. Students cannot email each other directly using their Office 365 account
- Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on Castle Court School website and only official email addresses should be used to identify members of staff

Social Media - Protecting Professional Identity (please see separate Social Media Policy)
Castle Court School provides the following measures to ensure reasonable steps are taken to minimise risk of harm to pupils, staff, and CCS through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures, and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made to social media to pupils, parents / carers, or school staff
- They do not engage in online discussion on personal matters relating to members of Castle Court School community
- Personal opinions should not be attributed to Castle Court School
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information

Unsuitable / inappropriate activities
Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Castle Court School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Castle Court School policy restricts usage as follows: **User Actions**		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of Castle Court School or brings Castle Court School into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Castle Court School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing outside school network					X	
Use of public social media					X	
Use of public messaging apps					X	
Use of video broadcasting e.g., YouTube		X				
Use of AI services that have not been approved by the school					X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

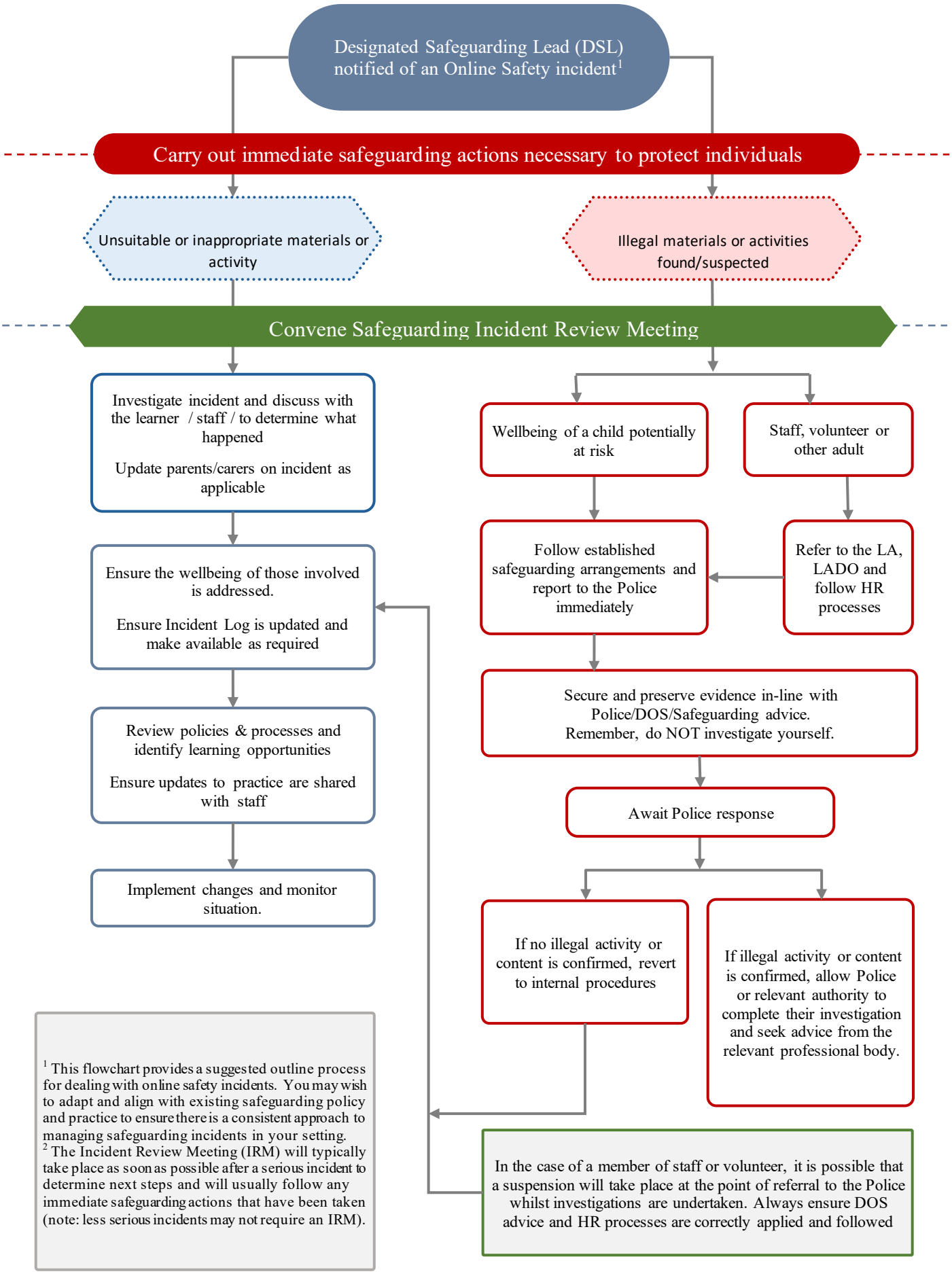
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include :
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:

- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Other Incidents
It is hoped that all members of Castle Court School community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Ransomware demands are covered in the anti-bribery policy

In the event of suspicion, all steps in this procedure should be followed, in conjunction with the 'Incident Management Tool'.

Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
Record the **URL** of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form (except in the case of images of child sexual abuse – see below)
Once this has been completed and fully investigated the investigating group of staff will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity, or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
The school has guidelines for initial responses to incidents of youth-produced sexual imagery. See Child Protection Policy

It is important that all the above steps are taken as they will provide an evidence trail for Castle Court School and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the investigating group for evidence and reference purposes.

School Actions & Sanctions
Staff
All adults working with children and young people have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. It is therefore expected that they will adopt very high standards of personal conduct to maintain the confidence and respect of the public in general and all those with whom they work. (Please see CCS: Code of Conduct for Staff Policy)

Pupils

It is more likely that Castle Court School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of Castle Court School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. (Please see Behaviour, Discipline and Exclusion policy.)

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- **We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR**
- **We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities**.
- **We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.**
- **As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.**
- **Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.**
- **Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.**
- **We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.**
- **The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.**
- **AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.**
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- *The school will support parents and carers in their understanding of the use of AI in the school AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI*

- *Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.*
- *We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.*
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Acknowledgements
CCS would like to acknowledge SWGfL for their e-Safety template which has been used in developing this policy. CCS also acknowledges a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of SWGL School e-Safety Policy Template and of the 360 Degree safe e-Safety Self Review Tool.

Appendix 1: Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Castle Court School will be responsible for ensuring that the school *infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within Castle Court School's policies)
- access to personal data is securely controlled in line with CCS Data Protection Policy (Personal Data)
- logs are maintained of users' system access
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders, and these have impact on policy and practice

Responsibilities

The management of technical security will be the responsibility of the Network Manager

Domain Security

The school's domain names are managed by RM using O365. The domains have DNS records set up for DKIM and DMARC recording.

Technical Security

Policy statements

Castle Court School will be responsible for ensuring that school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that Castle Court School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school's technical systems
- Servers, wireless systems, and cabling (wherever possible) must be securely located and physical access restricted and must be given a high priority for any future school wide IT Network development
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of Castle Court School systems and data

- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- All users will have clearly defined access rights to school technical systems. *Access rights available to groups of users are maintained by the Network Manager.*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place. Castle Court School uses Mosyle for the management of mobile devices and security
- School technical staff regularly monitor and record the activity of users on Castle Court School technical systems and users are made aware of this in the Acceptable Use Agreement
- Where appropriate, remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Network Manager
- The downloading of executable files and the installation of programmes on school devices by users is prohibited. However, any requests will be considered by the Network Manager
- An agreed policy is in place, please refer to the CCS Staff User Agreement, regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school
- Pupils and Staff are not allowed to use any form of removable media. Please refer to the CCS Data Protection Policy, regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on school devices
- Castle Court School infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data must not be sent over the internet or taken off Castle Court School site unless safely encrypted or otherwise secured. Please refer to the CCS Data Protection Policy.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. All school networks and systems are protected by secure passwords that are regularly changed
- The "master / administrator" passwords for Castle Court School systems, used by the technical staff is also available to the Head of ICT and is kept in a secure place

- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Department or teaching staff where appropriate
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will change their passwords annually – as described in the staff and student / pupil sections below.
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account

Staff passwords:

- All staff users will be provided with a username and password by the IT Department who keeps an up-to-date record of users, and their usernames must not include proper names or any other personal information about the user that might be known by others
- Temporary passwords e.g., used with new user accounts or when users have forgotten their passwords, are enforced to change immediately upon the next account log-on passwords shall not be displayed on screen, and are securely hashed (use of one-way encryption)
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords should be significantly different from previous passwords (*the last four passwords must not be re-used*) created by the same user.

Student / pupil passwords

- All users at KS2 and above will be provided with a username and password by the IT Department who will keep an up-to-date record of users and their usernames. Users at KS1 and below will be provided with a username and a group specific password
- Pupils will be taught the importance of password security

Training / Awareness

Members of staff will be made aware of Castle Court School's password policy:

- at induction
- through the Acceptable Use Agreement

Pupils will be made aware of Castle Court School's password policy:

- in lessons
- through the Responsible Use Policy

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- User Ids
- User log-ons
- Security incidents related to this policy

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-Safety and acceptable use. It is important that Castle Court School has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- a member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.

Responsibilities
The responsibility for the management of Castle Court School's filtering policy will be held by the Head of ICT and RM Network Manager. They will manage Castle Court School filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person, Head
- be discussed and authorised by the Head
- be reported to the e-Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the IT Department any infringements of Castle Court School's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements
Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by Castle Court School. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts Castle Court School to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through Castle Court School network, filtering will be applied that is consistent with school practice.

- Castle Court School maintains and supports the managed filtering service provided by the Internet Service Provider (SWGfL/RM), Ripple and Smoothwall

- Castle Court School has provided enhanced / differentiated user-level filtering using the Smoothwall filtering programme. (Allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of ICT
- Mobile devices that access Castle Court School internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on Castle Court School systems
- Any filtering issues should be reported immediately to the IT Department or the filtering provider when appropriate
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Support Team and Head of ICT If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the e-Safety Group

Education / Training / Awareness
Pupils will be made aware of the importance of filtering systems through the e-Safety Education Programme: Computing lessons, CAVE sessions and external Internet Safety sessions they will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:
- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset

Parents will be informed of Castle Court School's filtering policy through the Acceptable Use Agreement and through e-Safety awareness sessions / newsletter etc.

Changes to the Filtering System
In this section Castle Court School should provide a detailed explanation of:
- how, and to whom, users may request changes to the filtering
- the grounds on which they may be allowed or denied access
- how a second responsible person will be involved to provide checks and balances
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to a responsible adult who will decide whether to make a request to the IT Department for a school level change.

Monitoring
The DfE Technical Standards for Schools and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

No filtering system can guarantee 100% protection against access to unsuitable sites. Castle Court School will therefore monitor the activities of users on Castle Court School network and on school equipment as indicated in Castle Court School E-Safety Policy and the Acceptable / Responsible Use Policy.

Monitoring will take place as follows:
- All internet traffic is monitored and logged through Smoothwall. The Network Manager regularly checks logs and reports any inappropriate usage to the e-Safety Coordinator. If Smoothwall identifies inappropriate use by a member of staff, an email will be sent to the Head. If Smoothwall identifies inappropriate use by a student in year 3 & 4 Mr A Laidler will be emailed, for 5 & 6 Mrs L Munns and for years 7 and 8 Ms K Thompson will be emailed. Mr P Dunsford will receive emails for all student's inappropriate use. The incidents will be investigated, and sanctions may be issued.

- In addition, all workstations on the school network are monitored by Securus. Securus captures keystrokes, indecent images and language used not only on the internet but in any application. A daily report is sent to the Head of IT, showing captures with a severity rating higher than 3.
- The police's Data Collector is configured on our main server. This collects any suspicious traffic and then produces a monthly report based on all the information collected from all its schools.
- Ripple is a browser extension that has been added to all windows devices in the school. It helps prevent self-harm and suicide by redirecting users to mental health resources when they search for harmful online content.
- A report of all Securus and Smoothwall activity will be presented in each Education Committee meeting.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person, Head of ICT
- e-Safety Group
- External Filtering provider / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage"

The 'Cyber-security in schools: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks

- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Computer Misuse and Cyber Choices Policy Template

All key stakeholders, including the school IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. This often happens without the individual even realising, young people need support in making the right #CyberChoices in their use of technology. Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years. The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the NCA Hacking it Legal Leaflet*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the NCA Cyber Choices site.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made (contact details for all Regional Organised Crime Units are available in the "what to do if you're concerned" section at the bottom of the NCA Cyber Choices page). Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Information for parents about NCA Cyber Choices available on the school website.

Appendix 2 Third party data sharing agreement.

CASTLE COURT SCHOOL

GENERAL DATA PROTECTION REGULATION

DATA PROCESSING AGREEMENT

Castle Court School IS CONTROLLER AND _____ PROCESSOR

BACKGROUND

This agreement is to outline the use of data between Castle Court School and _____ for the sole purposes of communicating via _____ to Castle Court parents about _____ lessons at Castle Court School. All data remains the property of Castle Court School and permission is not granted for any other use other than communicating about tennis lessons at Castle Court School.

(A) This Agreement is to ensure the protection and security of Personal, including all Personal Data passed from the school (Data Controller) to the Supplier (Data Processor) for processing, or accessed by the Supplier on the School's authority for processing, or otherwise received by the Supplier for processing on the school's behalf.
(B) The Data Protection Laws place certain obligations upon a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the processing of the Personal Data carried out on its behalf is secure.
(C) This Agreement exists further to ensure that there are sufficient security guarantees in place and that the processing complies with obligations equivalent to those required by the Data Protection Laws.
(D) This Agreement further defines certain service levels to be applied to all uses of Personal Data and all Personal Data related services provided by the Supplier.
(E) Definitions in this Background have the meanings given in the Agreement and/or the Data Protection Laws.

1. Data Protection

1.1 **Definitions**

In this Agreement:
Data means all Personal Data collected, generated, or otherwise processed by the Supplier as a result of, or in connection with, the provision of the Services.
Data Protection Laws means:

(a) prior to 25 May 2018, the Data Protection Act 1998.
(b) from 25 May 2018, the General Data Protection Regulation (EU 2016/679) (**GDPR**) and any legislation which amends, re-enacts or replaces it in England and Wales.
(c) the Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces it; and
(d) at all times, any other data protection laws, and regulations applicable in England and Wales.

[**Data Protection Officer** has the meaning given to it under Article 37 of GDPR.]
Data Subject means an individual who is the subject of personal data.
[**EEA** means the European Economic Area.]

[**Losses** means costs, claims, demands, actions, awards, judgments, settlements, expenses, liabilities, damages and losses (including all interest, fines, penalties, management time and legal and other professional costs and expenses).] **Personal Data** has the meaning given to it under the Data Protection Laws.

Records means the records referred to in Clause 1.7.1.
Services means provision of tennis lessons.
Services Agreement means for the duration of the provision of tennis lessons at Castle Court School.
Sub-Processor has the meaning set out in Clause 1.4.1.
Supervisory Authority means any data protection authority with jurisdiction over the processing of the Data.

1.2 Data Processing

1.2.1 _____ shall comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done which might lead to a breach by Castle Court School of the Data Protection Laws.

1.2.2 _____ may only process Data to the extent it relates to:

(a) the types of Data.

(b) the categories of Data Subject; (c) the nature and purpose, set out in Schedule [●] and

only for the duration specified therein.

1.2.3 Without prejudice to Clause 1.2.1 [_____] shall:

(a) process the Data only in accordance with the written instructions of Castle Court School, unless _____ is required to process. the Data for other reasons under the laws of the European Union (or a member state of the European Union) to which _____] is subject. If _____ is required to process the Data for these other reasons, _____ shall inform Castle Court School before carrying out the processing, unless prohibited by relevant law.

(b) immediately inform Castle Court School if it believes that Castle Court School's instructions infringe the Data Protection Laws.

(c) have in place, and always maintain throughout the term in accordance with the then current [best industry practice/good industry practice], all appropriate technical and organisational security measures against:

(i) unauthorised or unlawful processing, use, access to or theft of the Data; and

(ii) loss or destruction of or damage to the Data,

to ensure that _____'s processing of the Data is in accordance with the requirements of the Data Protection Laws and protects the rights of the Data Subjects. On request _____ shall provide Castle Court School with a current written description of the security measures being taken.

(d) ensure that all persons authorised by _____ to process Data are bound by obligations equivalent to those set out in this Clause 1.

(e) ensure that access to the Data is limited to:

(i) those _____ personnel who need access to the Data to meet _____ obligations under the Agreement; and

(f) in the case of any access by any _____ personnel, such Data as is strictly necessary for performance of that _____ personnel's duties.

(g) if required under the Data Protection Laws, appoint a Data Protection Officer.

1.2.4 _____ shall provide such assistance as Castle Court School requires for Castle Court School to:

(a) respond to requests relating to _____ data processing from Data Subjects.

(b) ensure compliance with Castle Court School's obligations under the Data Protection Laws, including in relation to:

(i) the security of processing; and

(ii) with the preparation of any necessary data protection impact assessments and the undertaking of any necessary data protection consultations.

1.3 Sub-Processors

1.3.1 _____ shall not engage any third party, including a member of _____'s group, to carry out processing in connection with the Services (**Sub-Processor**) without Castle Court School's prior written consent. For the avoidance of doubt, this Clause 1.4.1 shall also apply to any replacement Sub-Processor.

1.3.2 Prior to allowing a Sub-Processor authorised in accordance with Clause 1.4.1 to process any Data, _____ shall enter into a written agreement with the Sub-Processor under which Sub-Processor is obliged to comply with the terms of this Clause 1. _____ remains fully liable to Castle Court School for any acts or omissions of any Sub-Processors.

1.4 Information Provision and Data Protection Audits

1.4.1 On request and at no additional charge, _____ shall provide to Castle Court School all information required by Castle Court School to assess _____'s compliance with Clause 1 and the Data Protection Laws and, to the extent possible, all information necessary for Castle Court School to demonstrate Castle Court School's compliance with the Data Protection Laws; and

1.4.2 In order that Castle Court School [and/or its authorised representative] and any Supervisory Authority may audit _____'s compliance with the Data Protection Laws and the terms of this Clause 1, on request and at no additional charge _____ shall provide Castle Court School with:

(a) reasonable access to all relevant information, premises, Data, employees, agents, _____ Sub-Processors, and assets at all locations from which obligations of [Supplier{arty] under this Clause 1 are being or have been or should have been carried out; and

(b) all reasonable assistance in carrying out the audit,

during the Term and for [36] months after the Termination Date, subject to Castle Court School giving _____ [five] [Business Days']/ [seven days'] notice (except where such audit is required by a Supervisory Authority to which Castle Court School is subject).

1.5 Dealings with Supervisory Authorities

1.5.1 _____ shall promptly provide all assistance and information which is requested by any Supervisory Authority.

1.5.2 _____ shall immediately notify Castle Court School of any request that it receives from any Supervisory Authority for assistance or information, unless prohibited by relevant law.

1.6 Records

1.6.1 _____ shall maintain records of all processing activities carried out on behalf of Castle Court School, including: (a) the information described in Clause 1.5.

(b) where applicable, the name and contact details of the Data Protection Officer [or representative based in the European Union] of _____ and of any sub-processors.

(c) the different types of processing being carried out (if applicable).

(d) any transfers of Data outside of the EEA [or UK], including the identification of the relevant country or international organisation and any documentation required to demonstrate suitable safeguards.

(e) a description of the technical and organisational security measures referred to in Clause 1.2.3, together, the Records (**Records**).

1.6.2 The Records shall be in written electronic form.

1.6.3 _____ shall provide the Records to Castle Court School promptly on request.

1.7 Data Subjects

On request, _____ shall take all necessary action and provide Castle Court School with all reasonable assistance necessary for Castle Court School to comply with Castle Court School's obligations under the Data Protection Laws in relation to:

1.7.1 the provision of information to Data Subjects.

1.7.2 the rectification of inaccurate Data in relation to a Data Subject.

1.7.3 the erasure of a Data Subject's Data; and

1.7.4 the retrieval and transfer of the Data of a Data Subject.

1.8 Data Breaches

1.8.1 _____ shall notify Castle Court School immediately after becoming aware of any unauthorised or unlawful processing, use of, or access to the Data, or any theft of, loss of, damage to or destruction of the Data (**Security Incident**) or any breach of this Clause 1. [Failure to notify Castle Court School shall be deemed a material breach of the Service Agreement under Clause [●] incapable of remedy.]

1.8.2 [In the event of a Security Incident, _____ shall provide Castle Court School with full co-operation and assistance in dealing with the Security Incident, in relation to:

(a) resolving any data privacy or security issues involving any Data; and

(b) making any appropriate notifications to individuals affected by the Security Incident or to a Supervisory Authority.

1.8.3 _____ shall investigate the Security Incident in the most expedient time possible and shall then provide Castle Court School as soon as possible thereafter with a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, and any other information that Castle Court School may request concerning the Security Incident.

1.8.4 _____ shall take all steps necessary to prevent a repeat of the Security Incident and shall consult with and agree those steps with the Castle Court School unless immediate steps need to be taken and it is impractical to consult with Castle Court School in that respect.]

1.9 Return or Destruction of Data

_____ shall, at Castle Court School's discretion, destroy or return all Data to Castle Court School on termination of this Agreement, and shall destroy or delete all copies it holds of the Data, unless relevant local law to which _____ is subject requires that Data to be retained.

1.10 Governing Law

If it is or becomes a requirement that, under the Data Protection Laws or other Applicable Laws, Clause 1 must be governed by the laws of a member state of the European Union, and the governing law specified in Clause [●] does not or ceases to satisfy this requirement, Clause 1 shall be governed by and construed in accordance with the laws of [●].

1.11 [**Warranties**

1.11.1 The Supplier (Data Processor) warrants that:

(a) it will process the Data in compliance with all applicable laws, enactments, regulations, orders, standards, and other similar instruments, including the Data Protection Laws; and

(b) it will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Data and against the accidental loss or destruction of, or damage to Data to ensure the school's compliance with the Data Protection Laws.

(c) The Supplier shall notify the school immediately if it becomes aware of:

(d) any unauthorised or unlawful processing, loss of, damage to or destruction of the Data.

(e) any advance in technology and methods of working which mean that the school should revise the security and technical measures in place to protect the Data as well as the processing of the Data.

1.11.2 The Data Controller (School) warrants that:

(a) it will provide the Supplier with all Data in compliance with all applicable laws, enactments, regulations, orders, standards, and other similar instruments, including Data Protection Laws; and

(b) the Data which it supplies or discloses to the Supplier, has been obtained fairly and lawfully; and

(c) it will obtain all necessary consents from persons whose Data is being processed and registrations with authorities to permit the school to transfer Personal Data to third parties pursuant to its obligations under this Agreement.]

1.12 Indemnity

_____ shall on demand indemnify Castle Court School from and against all Losses incurred by Castle Court School [or any member of its Group or any of their respective] [, [its]] employees, officers, agents and contractors] as a result of any breach by _____ (or any entity or individual appointed by _____ to carry out its obligations) of Clause 1.

1.13 Priority

_____ shall comply with this Agreement in addition to its obligations under any other contract with the Castle Court School (whether currently in force or entered in the future). Where there is any inconsistency between the two, in relation to [data protection law] [confidential information] this Agreement shall prevail, unless the Castle Court School notifies the _____ otherwise in writing.

Signed on behalf of _____ (Poole)

Sign _____

Print _____

Date _____

Signed on behalf of Castle Court School

Sign _____

Print _____

Date _____

Appendix 3:

Staff Photography / Videography Declaration

As part of the school's ongoing commitment to child protection, it is not normal for colleagues to make or store images (including videos) of children using their own photographic equipment (cameras or phones) as part of their usual professional duties. No visiting members of staff have permission to photograph or film Castle Court pupils unless they are employed specifically to do so.

However, on occasions, there may be reasons for permitting such use. All colleagues (or approved external providers) are required to sign this declaration ahead of any such use, and gain prior permission from the Head, whether they are taking photos as part of a specific photographic project/assignment or managing a social media channel. Only staff with prior permission from the Head are permitted to use their phones/photographic equipment for school purposes.

I understand that:

- Any images I take must only be used for school purposes.
- Permission will not be given for photography involving swimming or situations in which children may be in a state of undress.
- Should I use my personal phone, photos must be uploaded to the school network or social media channel as soon as possible and then deleted from the phone's memory/photo stream (including 'recently deleted'). The school reserves the right to check photo streams on phones to ensure that school related photos have been deleted.
- Should I use my own camera the school will provide a memory card. The card should not be used for any personal reasons.
- Where possible, any editing of images should be done on site, with all images transferred to the school's network. If photos are used for social media they must, once uploaded, be deleted from personal devices (including 'recently deleted').
- If any editing of the images is to be performed away from school, images may only be stored on school devices.
- I am not permitted to keep any files in storage away from Castle Court (and its network) for possible use in future projects.
- Some parents have specifically asked for their children's images not to be used in school publicity or on social media: I have a responsibility to check the list of such pupils prior to putting together any publicity material for the school and ensure that any such pupils are not identifiable in the images used.
- All work of this nature remains the property of Castle Court School and may not be used for publicising other organisations without permission, in advance, from the Head.
- I shouldn't identify any pupils on social media with their first and surnames: I will only refer to pupils by their first names.
- At Castle Court we have a 'challenge' culture where any member of the community can challenge me as to why I am taking images of children; on such occasions, I will respond appropriately by informing the colleague/pupil/parent the reasons for the photos being taken.
- Where possible I should initiate conversation with those being photographed so that they know that the photos are being taken and how they will be used; if a pupil expresses unease about this, I should stop taking photos and discuss the issue further with them.
- Where photos are taken during residential school trips (eg Activities Week) it may not be possible for photos to be uploaded to the school network whilst away from school; in such instances, I should endeavour to remove all photos from my device (included 'recently deleted') within 24 hours of the trip's return to school.