Online Safety Policy

Title	Online Safety Policy
Author/Owner	Trust Board
Status	Final - Approved
Ratified Date	September 2024
Ratified by	Trust Board
Staff Consultation Date	N/A
Review Cycle	Annual
Review Date	September 2025
Security Classification	OFFICIAL

Version Control

Date of Change	Author	Detail of Change
Mar-22	T Nash	New DET Policy
Jan-23	T Nash	Several changes to Roles and Responsibilities. KCSiE 2021 amended to 2022. Personnel changes reflected in Key Contacts section. New related documents added. One new link added in Useful Links and Resources section.
Jul-23	T Nash	Section 12. Strengthened wording regarding use of personal devices to take photos and videos of pupils.
Jan-24	T Nash	Sections 4, 5 and 7 updated to reflect KCSiE focus on filtering and monitoring. Section 15 updated to include current contact detail and to add HPS and KHCPS.
Jun-24	T Nash	Section 15 updated to reflect personnel changes.
Sep-24	T Nash	Various cosmetic changes and addition of Generative AI clause.

Contents

1. Overview

This Policy is based on the London Grid for Learning (LGfL) DigiSafe template.

2. Aims

This Policy aims to:

- Set out expectations for all members of the Discovery Educational Trust (DET) and its Schools' community (including all staff, Members, Trustees, Local Governors, volunteers, contractors, pupils, parents/carers, visitors and community users) online behaviour, attitudes and activities and the use of digital technology (including when devices are offline).
- Help Safeguarding teams and Senior Leadership Teams (SLTs) to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the School gates and School day, regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help DET/School employees, working with children, to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care;
    - for their own protection, minimising misplaced or malicious allegations, and to better understand their own standards and practice;
    - for the benefit of DET/its Schools, supporting the ethos, aims and objectives of DET/its Schools, and protecting the reputation of DET/its Schools and the teaching profession;
- establish clear structures by which online misdemeanours are treated, and procedures to follow where there are doubts or concerns (with reference to related policies).

3. Scope

This Policy applies to all members of the DET/Schools' community (including staff, Members, Trustees, Local Governors, volunteers, contractors, pupils, parents/carers, visitors and community users), who have access to digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their School/Trust role.

4. Roles and Responsibilities

Each DET School is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning, and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of DET and its Schools.

In 2024/25, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Headteacher

Key Responsibilities

- Foster a culture of safeguarding where online safety is fully integrated into whole-School safeguarding;
- Oversee the activities of the Safeguarding Team, and ensure that the Designated Safeguarding Lead (DSL) responsibilities listed below are being followed and fully supported;
- Ensure that policies and procedures are followed by all staff;
- Undertake training in online and offline safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance;
- Liaise with the DSL on all online safety issues, which might arise, and receive regular updates on School issues and broader policy and practice information;
- Take overall responsibility for data management and information security ensuring that the School provision follows best practice in information handling; working with the Data Protection Officer (DPO), DSL, Trust Board (TB) and Local School Committee (LSC) to ensure compliance with General Data Protection Regulation (GDPR) legislation for storing data, but helping to ensure that child protection is always placed first and that Data Protection processes support careful and legal sharing of information;
- Ensure that the School implements and makes effective use of appropriate Information and Communications Technology (ICT) systems and services, including School-safe filtering and monitoring, protected email systems, and that all technology, including cloud systems, are implemented according to "child safety first" principles;
- Better understand, review and drive the rationale behind decisions in filtering and monitoring in accordance with Department for Education (DfE) standards, through regular liaison with IT colleagues and the DSL, and, in particular, understand what is blocked or allowed for whom, when and how (as per KCSiE).
- Be responsible for ensuring that all staff receive suitable training (including online safety) at induction and with regular updates in order to carry out their safeguarding and online safety roles;
- Ensure that Local Governors are regularly updated on the nature and the effectiveness of the School's safeguarding and child protection arrangements;
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident;
- Support the Safeguarding Team and technical staff as they review protections for pupils in the home, and remote learning procedures, rules and safeguards;
- Assign responsibility to a nominated member of staff to undertake online searches, with consistent guidelines, as part of due diligence for the recruitment shortlist process;
- Ensure suitable risk assessments are undertaken in order for the curriculum to meet the needs of pupils, including the risk of children being radicalised;
- Ensure that there is a system in place to monitor and support staff, e.g. the Network Manager, who carries out technical procedures related to online safety;
- Ensure that the School website meets statutory DfE requirements. This responsibility is delegated to the DET Director of Operations.

Designated Safeguarding Lead/Online Safety Lead

Key Responsibilities

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)."
- Where the Online Safety Lead (OSL) is not the named DSL, ensure that there is regular review and open communication between these roles, and that the DSL's clear overarching responsibility for online safety is not compromised;
- Work with the HT and technical staff to review protections for pupils in the home, and remote learning procedures, rules and safeguards;
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.";
- Ensure that all staff complete safeguarding and child protection training (including online safety) at induction, and that this is regularly updated;
- Liaise with the HT and the Chair of the Trust Board and Local School Committee to ensure that all Trustees and Local Governors complete safeguarding and child protection training (including online safety) at induction, to enable them to provide strategic challenge and oversight into policy and practice, and that this is regularly updated;
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language;
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply;
- Work closely with the Trust, SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the School);
- Establish an online safety group, comprising a range of stakeholders: DSL/OSL, Local Governors, pupils (via views or direct membership), to plan and embed an online safety strategy;
- "Liaise with the local authority and work with other agencies in line with 'Working Together to Safeguard Children'" (DfE);
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- Work with the Headteacher (HT) (if relevant), DPO and LSC to ensure a GDPR-compliant framework for storing data, but help to ensure that child protection is always put first and Data Protection processes support careful and legal sharing of information;
- Stay up-to-date with the latest trends in online safety;
- Review and update this Policy and other related documents, e.g. acceptable use documentation, to ensure a joined-up approach to online safety;
- Receive regular updates in online safety issues and legislation, be aware of local and School trends;

- Ensure that online safety education is embedded across the curriculum, e.g. by use of the UK Council for Child Internet Safety (UKCCIS) framework 'Education for a Connected World', and beyond, in wider School life;
- Promote an awareness and commitment to online safety throughout the DET/School community, with a strong focus on parents/carers, including hard-to-reach parents/carers;
- Liaise with School Technical, Pastoral, and Support Staff, as appropriate;
- Communicate regularly with Senior Leaders and the LSC to discuss current issues (anonymised), review incident logs and discuss the effectiveness of filtering and monitoring;
- Ensure that all staff are aware of the procedures that they should follow in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident;
- Ensure adequate provision for staff to flag issues when not in School, and for pupils to disclose issues when off-site, especially when in isolation/quarantine/lockdown;
- Oversee and discuss "appropriate filtering and monitoring" (physical or technical) with LSC, and ensure that staff are aware that these safeguards are in place;
- Ensure that all staff read 'Keeping Children Safe in Education' Parts 1 and 5;
- Cascade knowledge of risks and opportunities throughout the School and wider DET.

Trust Board, led by Link Trustee for Safeguarding

Key Responsibilities

- Approve this Policy and strategy, and subsequently review its effectiveness;
- Complete (and signpost all other Trustees and Local Governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge to policy and practice, ensuring that this is regularly updated;
- With the Central Trust team, ensure that all other Trustees and Local Governors complete safeguarding and child protection training (including online safety) at induction and annually thereafter;
- Ensure that an appropriate member of each School's Senior Leadership Teams (SLT), is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority;
- Support the Schools in encouraging parents/carers and the wider community to become engaged in online safety activities;
- Have regular strategic reviews with the OSLs/DSLs, and incorporate online safety into standing discussions of safeguarding at TB and LSC meetings;
- Where the OSL is not the named DSL, ensure that there is regular review and open communication between these roles;
- Work with the DPO, DSLs and HTs to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and Data Protection processes support careful and legal sharing of information;
- Check that all DET/School staff have read Parts 1 and Annex B of 'Keeping Children Safe in Education 2024';
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and are regularly updated in line with advice from the LSCB;

- Ensure that appropriate filters and appropriate monitoring systems are in place, but be mindful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding;
- Ask about how the Schools have reviewed protections for pupils at home (including when with online tutors) and remote learning procedures, rules and safeguards;
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole School approach to online safety with a clear policy on the use of mobile technology.";
- Support the Schools in encouraging parents/carers and the wider communities to become engaged in online safety activities.

All Staff

Key Responsibilities

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up;
- Know who your OSL and DSL are;
- Read Parts 1 and Annex B of 'Keeping Children Safe in Education 2024';
- Read and follow this Policy in conjunction with DET's Safeguarding and Child Protection Policy;
- Record online safety incidents in the same way as any safeguarding incident, and report it in accordance with School procedures;
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece, so do not keep anything to yourself;
- Sign and follow the Acceptable Personal Use of Resources and Assets Policy and Code of Conduct;
- Notify the OSL/DSL if policy does not reflect practice in your School and follow escalation procedures if concerns are not promptly acted upon;
- Identify opportunities to thread online safety through all School activities, both outside the classroom and within the curriculum, supporting curriculum/stage/ subject leads and making the most of unexpected learning opportunities as they arise;
- Whenever overseeing the use of technology in School or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites;
- Follow best practice pedagogy for online safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods;
- Carefully supervise and guide pupils when engaged in learning activities that involve online technology, supporting them with search skills, critical thinking, e.g. fake news, age-appropriate materials and signposting, as well as legal issues such as copyright and data law;
- Encourage pupils to follow relevant acceptable use documentation, remind them about it and enforce School sanctions;
- When supporting pupils remotely, be mindful of additional safeguarding considerations;
- Be aware of security best practice at all times, including password hygiene and phishing strategies;
- Notify the OSL/DSL of new trends and issues before they become a problem;

- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter. This includes bullying and harmful sexual behaviour. Refer also to the DET Harmful Sexual Behaviour/Child-on-Child Abuse Policy.
- Be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and harmful sexual behaviour) in the playground, corridors, toilets and other communal areas outside the classroom – let the OSL/DSL know;
- Receive regular updates from the OSL/DSL and have a healthy curiosity for online safety issues;
- Model safe, responsible and professional behaviours in the use of technology. This includes outside of the School's operating hours, offsite and on social media, in all aspects upholding the reputation of DET/School and the professional reputation of all staff.

Personal, Social, Health and Economic (PSHE) Education Leads

Key Responsibilities effective September 2020 in accordance with Government Guidance on Personal, social, health and economic education.

As listed in the 'All Staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE/Relationships and Sex Education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" to complement the computing curriculum.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSE Policy should be included on each School's website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Curriculum Lead(s)

Key Responsibilities

As listed in the 'All Staff' section, plus:

- Oversee the delivery of the online safety element of the computing curriculum in accordance with the National Curriculum;
- Work closely with the PSHE Education Lead to avoid overlap, but to ensure a complementary whole-School approach;
- Work closely with the OSL/DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing;
- Collaborate with technical staff and others responsible for ICT use in the Schools to ensure a common and consistent approach, in line with acceptable use documentation.

Subject Leaders

Key Responsibilities

As listed in the 'All Staff' section, plus:

- Look for opportunities to embed online safety in your subject and model positive attitudes and approaches to staff and pupils alike;
- Consider how the UKCCIS framework 'Education for a Connected World' can be applied in your context;
- Work closely with the OSL/DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

Network Manager/IT Technician

Key Responsibilities

As listed in the 'All Staff' section, plus:

- Keep up-to-date with DET's Online Safety Policy and technical information in order to effectively carry out the online safety role and inform and update others as relevant;
- Ensure that the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal data, web filtering settings, sharing permissions for files on cloud platforms etc.);
- Collaborate regularly with the DSL and SLT to help them make key strategic decisions around the safeguarding elements of technology and its role in safeguarding;
- Support the Trust, the DSL and SLT to undertake an annual online safety audit as recommended by KCSiE;
- Support and advise on the implementation of appropriate filtering and monitoring as decided by the OSL/DSL and SLT;
- Maintain up-to-date documentation of DET/School online security and technical procedures;
- Report online safety-related issues that come to their attention in line with DET/School policies;
- Manage the DET/School systems, networks and devices, according to a strict password policy, with systems in place to detect misuse and malicious attack, with adequate protection, encryption and backup of data, including disaster recovery plans, and auditable access controls;

- Monitor the use of DET/School technology and online platforms and ensure that misuse/attempted misuse is identified, reported and managed in line with DET/School policy;
- Work with the HT and the Trust Director of Operations to ensure that the DET/School website meets statutory DfE requirements.

Data Protection Officer (DPO)

Key Responsibilities

- Alongside those of other staff, provide Data Protection expertise and training and support the Data Protection Policy and Cyber Response Plans and compliance with those and legislation and ensure that the policies conform with each other and with this Policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and Contractors

Key Responsibilities

- Read, understand, sign and adhere to acceptable use documentation;
- Report any concerns, no matter how small, to the OSL/DSL;
- Maintain an awareness of current online safety issues and guidance;
- Model safe, responsible and professional behaviours in their own use of technology at School and as part of remote teaching or any online communications.

Pupils

Key Responsibilities

- Read, understand, sign and adhere to relevant acceptable use documentation;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials;
- Know what action to take if they, or someone they know, feels worried or vulnerable when using online technology;
- Treat home learning during any isolation/quarantine or lockdown in the same way as regular learning in School and behave as if a teacher or parent/carer were watching the screen;

- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with School staff or tutors;
- Share views with the online safety group (either as direct members or via feedback/survey responses) in order to assist with the formulation and implementation of an online safety strategy;
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of the School, and realise that the School's acceptable use documentation covers actions out of School, including on social media;
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at School or outside of School if there are problems.

Parents/Carers

Key Responsibilities

- Read, sign and promote the relevant acceptable use documentation, and read the pupil acceptable use documentation and encourage their children to follow it;
- Consult with the School if they have any concerns about their children's use of technology;
- Promote positive online safety, and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative or threatening comments about others, including members of the DET/School community.
- Encourage children to engage fully in home-learning, whether for homework or during any School closures or isolation, and flag any concerns;
- Support the child during any home learning to avoid video calls in a bedroom, if possible, and, if not, to ensure that the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc., and the background blurred or changed where possible;
- If organising private online tuition, remain in the room if possible, and ensure that the child knows that tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External Groups including Parent Associations

Key Responsibilities

- Any external individual/organisation signs relevant acceptable use documentation prior to using technology or the internet within DET/its Schools;
- Support DET/Schools in promoting online safety and Data Protection;
- Model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative or threatening comments about others, including members of the DET/School community.

5. Education and Curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE/RSE;
- Computing;
- Citizenship.

However, it is the role of all staff to identify opportunities to thread online safety through all of the School's activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology in the School or setting a homework task, all staff should encourage sensible use and consider potential dangers as well as the age appropriateness of websites (ask the OSL/DSL what appropriate filtering and monitoring policies are in place).

"Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online. "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online." (KCSIE 2024).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, e.g. fake news, age-appropriate materials and signposting as well as legal issues such as copyright and data law.

DET and its Schools recognise that online safety and broader digital resilience must be threaded throughout the curriculum.

Annual reviews of curriculum plans/schemes of work (including for Special Educational Needs and Disabled (SEND) pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online Relationships, Online Reputation, Online Bullying, Managing Online Information, Health, Wellbeing and Lifestyle, Privacy and Security, and Copyright and Ownership.

6. Handling Online Safety Concerns and Incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSE and Citizenship.

General concerns must be handled in the same way as any other safeguarding concern; all stakeholders should talk to the OSL/DSL with even low-level concerns. This could contribute to the overall picture or highlight what might not yet be a problem.

Associate/Support Staff often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

DET's procedures for dealing with online safety are mostly detailed in the following policies:

- DET Safeguarding and Child Protection Policy;
- School Anti-Bullying Policy;
- School Behaviour Policy;
- School Cyber Response Plan;
- Acceptable use documentation;
- DET Data Protection Policy;
- DET Harmful Sexual Behaviour/Child-on-Child Abuse Policy;
- DET Searching, Screening and Confiscation Policy.

Each School commits to take all reasonable precautions to ensure online safety, but recognises that incidents occur both inside and outside of School (and that those from outside may continue to impact on pupils when they come into School). All members of the School are encouraged to report issues swiftly to allow them to be dealt with quickly and sensitively through the escalation processes.

Any suspected online risk or infringement should be reported to the OSL/DSL on the same day – where clearly urgent, it must be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the HT, unless the concern is about the HT, in which case the complaint is referred to the Chief Executive Officer (CEO) and the Local Authority's Designated Officer (LADO). Staff should also refer to the DET Procedure for Dealing with Safeguarding Allegations Against Adults in School and can also use the NSPCC Whistleblowing Advice Line.

The School actively seeks support from other agencies, as needed (i.e. the Local Authority (LA), RM SafetyNet, UK Safer Internet Centre's Professionals' Online Safety Helpline, National Crime Agency (NCA), Child Exploitation and Online Protection (CEOP) Command, Prevent Officer, police, Internet Watch Foundation (IWF)). Parents/carers are informed of online safety incidents involving their children. The police are contacted where staff or pupils engage in or are subject to behaviour, which may be considered particularly disturbing or breaks the law.

7. Appropriate Filtering and Monitoring

'Keeping Children Safe in Education' (KCSiE) obliges schools to ensure that "appropriate filtering and monitoring systems [are] in place, and regularly review their effectiveness." Furthermore, "that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding."

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the DSL now has lead responsibility for filtering and monitoring.

DET and its Schools must follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems;
- review filtering and monitoring provision, at least, annually;
- block harmful and inappropriate content without unreasonably impacting teaching and learning;
- have effective monitoring strategies in place that meet their safeguarding needs.

DET and its Schools use the internet connection provided by RM Education. This means that all Schools have a dedicated, secure, School-safe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

- Physical monitoring by staff watching the screens of users (adult supervision in the classroom, at all times);
- Live supervision by staff on a console with device management software;
- Network monitoring using log files of Internet traffic and web access;
- Individual device monitoring through software of third-party services.

Internet usage across DET and its Schools is recorded, thereby enabling reports to be run on individual users.

Filtering is applied at different levels across different user cohorts, i.e. pupils, staff and administrators, and pupils have the most stringent filters applied.

Pupil-level filtering is applied to all devices using Wi-Fi.

Both the DSL and members of the SLT should ensure that they better understand, review and drive the rationale behind decisions in this area. Technology teams and Safeguarding teams need to work much more closely together for this to be possible and technicians are responsible for undertaking regular checks and feeding information back to the DSL and the Safeguarding team.

All members of staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, the potential for pupils to bypass systems and any potential overblocking. DET/School staff can submit concerns at any point by raising a ticket with the appropriate IT Support Team, and are asked for feedback at the time of the regular checking process.

Staff are reminded of the systems in place and their responsibilities at induction and at the start of the academic year via safeguarding training as well as regular training reminders in the light of the annual review and regular checks that are undertaken.
At DET:

- web filtering and monitoring is provided by RM Education – RM Safetynet or Smoothwall;
- changes to the filtering can be made by local School IT Support Teams;
- overall responsibility is held by the DSL in each School;
- technical support and advice, setup and configuration guidance can be sought from local IT Support teams;
- checks are made half termly by local IT Support Teams to ensure that filtering is still active and functioning. The system is also monitored by the solution provider and notifications are sent if there are any issues;
- an annual review of each School is undertaken using '360 Safe' as part of the online safety audit to ensure a Trust-wide approach.

8. Password and Screen Lock Protocols

A Password Policy is enforced across all DET and School staff and system administrator accounts with the following requirements:

- Passwords must comprise a minimum of eight characters and must contain characters from each of the following groups: upper case characters, lower case characters, digits and special characters.
- A network enforced password change takes place every 90 days and prevents the user from using any of the last three passwords set.

Additionally, all computer monitors lock after a period of inactivity, thereby minimising the risk of misuse. The lock-out timing differs between teaching and non-teaching staff (60 minutes for teachers, ten minutes for non-teaching staff) to accommodate teachers being away from screens for longer periods, i.e. while standing and presenting to a class.

9. Communication

Email and messaging

- Pupils and staff at DET Schools use approved systems for all School emails (Microsoft Office 365).

These systems are managed by the Schools.

General principles for email and messaging are as follows:

- School email systems and messaging within learning environments managed by Schools are the only means of electronic communication to be used between staff and pupils or staff and parents/carers (in both directions). Any unauthorised use of a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the HT (if by a staff member). There should be no circumstances where a private email or messaging is used.
- Staff or pupil personal data should never be sent/shared/stored on email.
- If data needs to be shared with external agencies, encrypted email is enabled. Internally, staff should use the School's network, including when working from home, or a DET/School-managed platform.

- Appropriate behaviour is expected at all times, and the DET/School-managed systems should not be used to send inappropriate materials or language, which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring DET/its Schools into disrepute or compromise the professionalism of staff.
- Staff are allowed to use the email and messaging system for reasonable (not excessive, not during lessons) personal use, but should be aware that all use is monitored, their messages may be read, and the same rules of appropriate behaviour apply at all times. Profanity filters are applied Trust-wide to identify emails using inappropriate language, images, malware or inappropriate sites, which may be blocked and not arrive at their intended destination as a result.

10.Discovery Educational Trust and School Websites

DET and School websites are key public-facing information portals for the DET/School community (both existing and prospective stakeholders) with a key reputational value. The CEO, HT, TB and LSCs have given overall responsibility for the day-to-day updating of the content to trusted members of staff. The DfE has determined information, which must be available on all school websites.

Where staff submit information for the website, they are asked to remember:

- Schools have the same duty, as any person or organisation, to respect and uphold copyright law (schools have been fined thousands of pounds for copyright breaches). Sources must always be credited, and material only used with permission.
- Where pupil work, images or videos are published on the website, identities must be protected, and full names are not published (including in file names/metadata).

11.Cloud Platforms

The following principles apply:

- Privacy Notices inform parents/carers and children (13+) when and what sort of data is stored in the cloud;
- New cloud systems and what may or may not be stored in them are approved by the OSL/DSL in consultation with technical staff. This is noted in a Data Protection Impact Assessment (DPIA) and parental/carer permission is sought in line with GDPR requirements;
- Regular training ensures that all staff understand sharing functionality, and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such;
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen;
- Pupil images/videos are only made public with parental/carer permission;
- Only DET/School-approved platforms are used by pupils or staff to store pupil work;
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive, and those belonging to a managed educational domain).

At the start of each half-term, all DET/School staff are reminded to liaise with IT immediately a requirement for a new Cloud-based application is identified.

12.Digital Images and Video

When a pupil joins a DET School, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent).

Whenever a photo or video is taken/made, the member of staff taking it checks the latest records of parental/carer consent before using it for any purpose.

Images in public-facing materials - such as School websites and blogs - do not have any name attached. In exceptional circumstances, additional permission from parents/carers may be sought to allow pupils, shown in public-facing materials, to be identified with a first name only.

All staff are governed by their contract of employment and DET's Acceptable Personal Use of Resources and Assets Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. With permission from the HT, staff may on an exceptional basis, use personal phones to capture photos or videos of pupils, but these must be appropriate, linked to DET/School activities, taken without secrecy and not in a one-to-one situation, and always moved to DET/School storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos and videos are stored on the DET/School network in line with the Records Management retention schedule.

Parents/carers are reminded at appropriate times - e.g. before School productions - about the importance of not sharing images taken in School.

Pupils are taught to think about their online reputation and digital footprint, so all staff should be good adult role models by not oversharing.

Pupils are taught about how images can be manipulated in their online safety education programme, and also taught to consider how to publish for a wide range of audiences.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name and metadata of the file), that reveals the identity of others and their location. They are taught about the need to keep their data secure and what to do if they are subject to bullying or abuse.

13.Social Media

DET Schools manage and monitor their social media footprint carefully to know what is being said about the Schools and to respond to criticism and praise in a fair, responsible manner.

Staff responsible for managing social media accounts must follow the guidance in the LGfL/Safer Internet Centre online reputation management document.

Staff, Pupils' and Parents'/Carers' Social Media Presence

Social media (including apps, sites and games that allow sharing and interaction between users) is a fact of modern life. However, as stated in acceptable use documentation, which all members of the DET/School community sign, everybody is expected to behave in a positive manner, engaging respectfully with the School and each other on social media as they would face-to-face.

This positive behaviour can be summarised as not making any posts, which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring DET and its Schools or (particularly for staff) the teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent/carer chats, pages or groups.

If parents/carers have a concern about DET/its Schools, they are encouraged to contact the relevant School directly, and in private, to resolve the matter. If an issue cannot be resolved in this way, the DET Complaints Policy and Procedure should be followed. Sharing complaints on social media is unhelpful and can cause upset to staff, pupils and parents/carers, also undermining staff morale and the reputation of DET/its Schools, which is important for the pupils they serve.

Many social media platforms have a minimum age of 13, but the Schools deal with issues arising on social media with pupils under the age of 13. Parents/carers are asked to respect age ratings on social media platforms, wherever possible, and not encourage underage use.

Schools have to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help their pupils to avoid or cope with issues if they arise. Online safety lessons look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children, typically, learn most from the models of behaviour they see and experience, which is often from adults. Parents/carers can best support this by talking to their children about the apps, sites and games they use, with whom and for how long.

DET Schools have official social media accounts and respond to general enquiries, but ask parents/carers not to use these channels to communicate about their children.

DET/School-managed email and messaging are the official electronic communication channels between parents/carers and DET/its Schools, and between staff and pupils.

Pupils are not allowed to be 'friends' with or make a friend request to any member of staff, Member, Trustee, Local Governor, volunteers and contractors or otherwise communicate via social media. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the EHT/HT and should be declared upon entry of the pupil or staff member to the School.

Staff must not 'follow' public pupil accounts and pupils should not follow staff, Member, Trustee, Local Governor, volunteer or contractor public accounts. Any attempt to do so may be a safeguarding concern or a disciplinary matter and should be notified to the OSL/DSL (if by a child) or to the EHT/HT (if by a staff member).

Staff are reminded that they are obliged not to bring DET or the teaching profession into disrepute, and the easiest way to avoid this is to have the strictest privacy settings and avoid

inappropriate sharing and oversharing online. They should never discuss DET/its Schools or its stakeholders on social media and be careful that their personal opinions are not attributed to DET/its Schools or LA, bringing DET/its Schools into disrepute.

All members of the DET community are reminded that, in the context of social media, it is important to note the DET Privacy Notice regarding School Photos and Additional Activities and to ensure that permission is sought before uploading photographs, videos or any other information about other people.

The acceptable use documents, which all members of the DET community sign, are also relevant to social media activity, as is the DET Data Protection Policy.

14.Device Usage

Please read the following in conjunction with the DET Acceptable Personal Use of Resources and Assets Policy.

Personal Devices and Bring Your Own Device (BYOD) Policy

- **Pupils**, who carry a mobile phone for their own safety when travelling to and from School, must abide by the individual arrangements in their School. Any attempt to use a phone or other device in School without special permission, or to take illicit photographs or videos results in sanctions, including confiscation.
- **All staff, who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during School operating hours, unless there is a professional need to respond to notifications. Devices should not be used for personal reasons during teaching periods without permission from a member of SLT.
- **Volunteers, contractors, Members, Trustees, Local Governors** should leave their phones in their pockets. They should not be used in the presence of children, or to take photographs or videos. If this is required, e.g. for contractors to take photos of equipment or buildings, permission must be sought from a member of staff, and the HT must be notified. Photos/videos must only be taken in the presence of a member of staff.
- **Parents/carers** are asked to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and be reminded of the importance of not sharing images taken in the School. Urgent messages to pupils should be sent via the School Office and not to a pupil's mobile phone.

Network/Internet Access on Personal Devices

- **Pupils** are not allowed to connect to any School network on personally-owned devices.
- **Staff** have access to networked files/drives via a managed remote access service and are not allowed access to networked files/drives on personally-owned devices.
- **Volunteers, contractors, Trustees, Members and Local Governors** can, with the HT's permission, access a guest wireless network on personally-owned devices without access to networked files/drives.
- **Parents/Carers** are not allowed to connect personal devices to any DET/School network.

Trips/Events Away from School

Teachers on Educational Visits should send messages to parents/carers via the relevant School Office, or a School Trip Phone. In very exceptional circumstances, staff using their personal phone in an emergency, must ensure that the number is hidden to avoid a parent/carer or pupil accessing a teacher's private phone number using 141.

Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', and the DET Searching, Screening and Confiscation Policy, authorised staff have a statutory power to search pupils/property on School premises. This includes the content of mobile phones and other devices, for example, as a result of a reasonable suspicion that a device contains illegal or undesirable material.

15.Use of Generative Artificial Intelligence (AI)

DET/its Schools acknowledge that the use of generative AI platforms is becoming widespread and are aware of, and follow, the DfE's guidance on this.

In particular:

- They talk about the use of these tools with pupils, staff and parents/carers – their practical use as well as their ethical pros and cons.
- They are aware that there will be use of applications and exposure to AI creations on devices at home for some pupils – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in examinations, or to plagiarise and cheat is prohibited, and sanctions in accordance with the School's Behaviour Policy and relevant examination policies will be used for any pupil found doing so.

Refer also to the DET Generative Artificial Intelligence Policy.

16.Key Online Safety Staff

The nominated DET Safeguarding Trustee is Mr. Stephen Baines.

Chase High School

Headteacher: Mr. Matt Suttenwood

Designated Safeguarding Lead: Mr. Ashley Brien

Online Safety Lead: Mr. Mohammad Hassan

Local School Committee Safeguarding Governor: Mr. Arthur Evans

Computing Curriculum Lead: Mr. Mohammad Hassan

PSHE Lead: Ms. Jo Whitfield

Network Manager: Mr. Toby Bubb

Technician: Mr. Simon Aylward

Hogarth Primary School

Headteacher: Mr. Rob Watson

Designated Safeguarding Lead: Mr. Rob Watson

Online Safety Lead: Miss Katherine Clarkson

Local School Committee Safeguarding Governor: TBC

Computing Curriculum Lead: Ms. Katherine Clarkson

PSHE Lead: Ms. Clare Connor

Network Manager: Mr. Matt Petts (interim)

Technician: TBC

Kelvedon Hatch Community Primary School

Headteacher: Miss Victoria Townsend

Designated Safeguarding Lead: Miss Victoria Townsend

Online Safety Lead: Miss Victoria Townsend

Local School Committee Safeguarding Governor: TBC

Computing Curriculum Lead: TBC

PSHE Lead: Ms. Gill Walker

Network Manager: Mr. Matt Petts (interim)

Technician: TBC

Larchwood Primary School

Headteacher: Mr. Steve Bowsher

Designated Safeguarding Lead: Mrs. Dawn Jaycock

Online Safety Lead: Ms. Lucy Beard

Local School Committee Safeguarding Governor: Mrs. Lisa Wenham

Computing Curriculum Lead: Mrs. Kerry-Ann Hyde

PSHE Lead: Ms. Sophie Rimmer

Network Manager: Mr. Matt Calhoun

Technician: Mr. Matt Calhoun

St. Martin's School

Executive Headteacher: Mr. Jamie Foster

Designated Safeguarding Lead: Mrs. Georgina Tatman

Online Safety Lead: Mrs. Gaynor Wilson

Local School Committee Safeguarding Governor: Mrs. Cynthia Amo-Ameyaw

Computing Curriculum Lead: Mr. James Spencer

PSHE Lead: Ms Laura Harris

Network Manager: Mr. Matt Calhoun

Technicians: Ms. Jen Lidbury and Mr. Adam Demetriou

17.Related Documents

DET Safeguarding and Child Protection Policy

School behaviour and anti-bullying policies

School Cyber Response Plans

DET Staff Code of Conduct

School acceptable use documentation for Pupils, Parents/Carers, Staff/Volunteers (including Members, Trustees and Local Governors) and Contractor/Agency Staff

DET Data Protection Policy and Privacy Notices

DET Searching, Screening and Confiscation Policy

DET Harmful Sexual Behaviour/Child-on-Child Abuse Policy

18.Useful Links and Resources

Child Exploitation and Online Protection (CEOP) Safety Centre - https://www.ceop.police.uk/Safety-Centre/

Childline - https://www.childline.org.uk/

Tel: 0800 1111

Thinkuknow – https://www.thinkuknow.co.uk/

Internet Watch Foundation - https://www.iwf.org.uk/.

Get Safe Online - https://www.getsafeonline.org/.

NSPCC - https://www.nspcc.org.uk/keeping-children-safe/online-safety/.

Live my Digital - https://www.youtube.com/watch?v=OBg2YYV3Bts for pupils.

Live my Digital - https://www.youtube.com/watch?v=1A51ggI1Fos for parents/carers.

Parents' Ultimate Guide to TikTok (Commonsense Media) - https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-tiktok

TikTok application safety – What parents need to know (Internet Matters) - https://www.internetmatters.org/hub/esafety-news/tik-tok-app-safety-what-parents-need-to-know/

Coerced Online Child Sexual Abuse – helping parents and carers keep their children safer online - https://saferinternet.org.uk/online-issue/coerced-online-child-sexualabuse

Reference should also be made to School Online Safety webpages.