Online Safety Policy

Parkland

This policy applies to all members of Discovery Trust including staff, pupils, advisory board members, volunteers, parents, carers, visitors, and community users who have access to and are users of Trust digital technology systems, both in and out of the Trust. The policy will be adopted by all Discovery Schools in the Trust and localised to their situation.

Version number	1.0
Consultation groups	Central Executive Team, Ed Tech Team, Blended learning network, IT technicians and Headteachers
Approved by	Board of Trustees
Approval date	December 2021
Adopted by	Advisory board
Adopted date	20.1.22
Implementation date	January 2022
Policy/document owner	Trust Online Safety Lead
Status	Statutory
Frequency of review	Annually
Next review date	September 2022
Applicable to	All Discovery Schools

Document History

Version	Version Date	Author	Summary of Changes
V1.0	9th September 2021	Adam Lapidge – Online Safety Lead	*New policy prepared in line with:* ▪ *Keeping children safe in education -September 2021* ▪ *Working Together to Safeguard Children", 2018* ▪ *Ofsteds Review of Sexual Abuse and Colleges – June 2021*

Contents

1. Statement of Intent from model policy

Parkland Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

This policy is consistent with the legal duty and legislation guidance including:

- 'Keeping children safe in education – Statutory guidance for schools and colleges', September 2021 (KCSIE 2021)
- 'Working Together to Safeguard Children', 2018
- 'Ofsted: Review of Sexual Abuse in Schools and Colleges', 2021

2. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Online Safety DSL has overall responsibility for the school's approach to online safety, with support from the school's senior leadership team, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

3. Linked Policies

The Trust and school's statutory responsibility for online safety goes beyond this policy. This policy is one of a series in Parkland integrated online safety portfolio and should be read and actioned in conjunction with the policies as listed below:

- Acceptable Use policy (KS1 & KS2)
- Anti-Bullying Policy (including Cyberbullying)
- Document Retention Management Policy?
- GDPR Data Protection Strategy
- Mental Health and Wellbeing Policy
- Mobile Phone and Smart technology policy
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Pupil Behaviour Policy
- Social Media Policy
- Special Educational Needs and Disability Policy
- Home Learning Protocol Policy

Staff related Policies and Procedures:

- Acceptable Use policy
- Disciplinary Policy and Procedure
- Mobile Phone and Loaned Property Policy
- Staff handbook which includes Staff Code of Conduct
- Staff Wellbeing Policy
- Trust Platform Working document

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for Online Safety.

All parents sign an acceptable use policy on behalf of their children when they join the school and then re-sign annually. (**Appendix 2)**

4. Key Roles and Responsibilities

At Parkland we take a whole-school approach to online safety and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all staff and volunteers read and understand this policy and implement it consistently.

Appendix 1 contains more information on the roles and responsibilities of specific stakeholders in Discovery, including:

- Advisory board members and Trustees
- Trust Online Safety Lead
- Headteachers
- School Online Safety Lead DSL

- School IT technicians
- All staff
- Pupils

5. Online Safety in the curriculum

We want our pupils to take responsibility and act in a responsible way.

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 online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across all subjects where relevant. The online safety curriculum used is SWGfL Project Evolve and is broad, relevant and provides progression, with opportunities for creative activities.
Online safety will be provided in the following ways:

- The school uses a planned online safety curriculum (SWGfL Project Evolve) which is delivered through dedicated online safety lessons, as well as being reinforced through all parts of daily school life.
- Key online safety messages are reinforced as part of a planned programme of assemblies and themed Online-Safety focused weeks, including Internet Safety Day and Wellbeing Week.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools are required to ensure all devices have monitoring software on them that detects and alerts the school of any potential exposure to extremism.
- Pupil's will be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, staff will do their best to ensure that students/pupils are 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) 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 and be agreed by the school's Headteacher/SLT before actioned by the technical team.

6. Responding to Online Incidents

6.1 Responding to pupil incidents

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

6.2 Responding to staff incidents

Where a staff member misuses the school's IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. A flow chart in dealing with illegal activity (**appendix 3)** supports the school in taking the correct action.

7. Parent Awareness and working with the wider community

We understand that many parents and carers only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of children's online behaviour. 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.
The school will provide information and awareness to parents and carers through:

- Curriculum activities, themed online safety awareness weeks. High profile events/campaigns e.g Safer Internet Day and Wellbeing Week.
- Letters, school newsletters, school web site
- Discovery Live - Webinars
- Parent/carers evenings
- Parent workshops
- Online Safety assemblies

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

8. Staff Training

8.1 All staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events or as part of internal training from the Trust's Online Safety Lead.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- Staff are expected to read and understand the trust's platform working document which outlines the safe use of applications and platforms with pupils.

8.2 Trust Online Safety Lead DSL

It is essential that the Trust Online Safety Lead DSL receives additional training to support them in their role. This training will be done by:

- Attending advanced online safety training DSL training on an annual basis.
- Participating in online safety expert groups (SWGfL 360 Safe Assessor Programme).
- Attending expert external training sessions through various providers.
- Keeping up to date with latest legislation and policy changes.

8.3 Trustees and Advisory board members

Advisory Board members/trustees take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This will be offered through:

- Participation in Trust training sessions delivered by the Online Safety Lead through regularly advisory board meetings.
- Participation in Trust lead conferences for Advisory Board members with a focus on Online Safety.

9. Technical Systems

9.1 Infrastructure and devices

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This is done by ensuring:

- The school technical systems are managed by trained professionals to ensure that it meets the recommended technical requirements as set out by the Keeping Children Safe in Education document.
- There will be regular reviews and audits of the safety and security of school technical systems, this is to be covered by both the online safety audit, as well as a cyber-security audit.
- Wireless systems and cabling are securely located and physical access restricted where it is possible.
- The school server is cloud-based and access to these systems are only given to prohibited staff.
- All users will have clearly defined access rights to school technical systems and devices.
- All users from year 2 and above will be provided with a username and secure password by school IT technician who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password. IT technicians are responsible for both adding and removing users as they start and leave the school. The school will only use generic school logins for EYFS/Year 1.
- The "master/administrator" passwords for the school systems, used by the IT Technician, is documented, and kept in a secure data storage system where additional access is only prohibited to the trust's senior IT team.
- The Director of IT 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.
- 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 the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software (Sophos).
- Any temporary user or guests must sign the schools 'Using School Systems Acceptable Use Agreement' when entering the building. These are accepted are part of the signing in process using the school's sign in system.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school. All staff who are given a device must sign a loan device equipment form **(see appendix 4**) which outlines their responsibilities when using school equipment at home. It is the authority of only the headteacher/head of school to decide if a staff member requires a device to use at home. Any school device that is loaned to a pupil is for educational purposes, and a parent/carer must sign a loan agreement form (**see appendix 5).**
- School IT Technicians will be responsible for downloading executable files and installing programmes on school devices. School staff are not given administrator rights on school devices and therefore are unable to install own programs/apps.
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users is forbidden on school devices, except in exceptional circumstances which have been agreed by the Director of IT. School IT technicians will be required to use removable media for installations of applications only. Personal data

cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

9.2 Filtering and monitoring

The school will be responsible for ensuring that the school internet filtering is as safe and secure and users are actively monitored for misuse. The school will ensure the internet is safe to use by ensuring:

- Internet access is filtered for all users. Illegal content is filtered by the broadband provider by actively employing the Internet Watch Foundation CAIC list. Web filtering content lists are regularly updated by the provider and internet use is logged and regularly monitored by the school IT technician. Any changes to a user's filtering level must be approved by the headteacher before actioning.
- Internet filtering is in place to ensure that children are safe from terrorist and extremist material when accessing the internet. The school ensures all school devices are installed with monitoring software specifically to comply with the Counter Terrorism and Security Act 2015.
- The school has provided differentiated age-appropriate filtering levels for its pupils and staff, ensuring that any content is appropriate for their age. Custom filtering groups can be setup if necessary, for specific circumstances but this must be agreed by the headteacher and Trust Online Safety Lead.
- IT technicians regularly monitor and record the activity of users on the school systems and users are made aware of this in the acceptable use agreement. The Trust Online Safety Lead monitors the central trust staff online activity. Any misuse of systems is recorded on our technician monitoring log (**Appendix 6)** before being passed onto the school senior leadership team. In cases where there is persistent misuse of ICT systems, an online safety timeline case log will be used on a user-by-user basis. **(Appendix 6)**
- There is a robust and appropriate system in place for users to report any actual/potential technical incident/security breach to the relevant person.

10. Online Safety Concerns

10.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

10.2 Peer on peer abuse

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

The school will respond to all concerns regarding online peer-on-peer sexual abuse and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

10.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Pupils are less likely to report grooming behaviour because:

- The pupil believes they are talking to another child
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

10.4 Child sexual exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

10.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

10.6 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions about using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

11. Personal Devices

11.1 Pupils

Pupils in upper KS2 may bring mobile devices into school. Parents/Carers will need to complete an agreement that their child can bring a mobile phone into school. Pupils must hand their mobile device into the office (directly or via the class teacher) where it will be kept securely. Pupils are not allowed to use their mobile phone during the school day, this includes:

- Lessons
- Playtime/Lunchtime
- Clubs before or after school

Any breach of the mobile device agreement may trigger disciplinary action in line with the school behaviour policy and could result in confiscation of their device.

11.2 Staff

Staff members must not use a personal device (e.g., phones and tablets) throughout the school day, unless this is in their own break/lunch time. Staff are not permitted to take or store images of pupils or staff on their mobile device. Personal information is not to be stored on any personal device. Personal mobile phones must not be used to contact pupils or parents. During school outings nominated staff will have access to a school mobile phone which can be used for emergency or contact purposes.

12. Remote Learning

All remote learning is delivered in line with the school's Home Learning Protocol Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, senso monitoring software installed, has working audio and video and can download documents where appropriate. The school is not responsible for ensuring that devices that go home have strict filtering installed and this is the responsibility of the parent/carer to ensure safe use.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software and filtering, on devices not owned by the school.

13. Policy Monitoring and Review

This policy will be reviewed at least annually (as a minimum) and be updated as needed, so that it is kept up to date with safeguarding issues as they emerge and evolve, including lessons learnt. The policy will also be revised following any national or local updates, significant local or national safeguarding events and/or learning, and/or any changes to our own procedures.

Appendix 1: Roles and Responsibilities

To see a detailed list of the roles and responsibilities for all stakeholders, please click the link below:

Discovery Trust Roles and Responsibilities

Appendix 2: Pupil KS2 & KS1 Acceptable Use Policies

Discovery Trust Acceptable Use Policies

Appendix 3: Staff online safety incident flow-chart

Discovery Trust Staff online safety incident flow-chart

Appendix 4: Loaned Agreement Form (Staff)

Staff Loaned Agreement Form

Appendix 5: Loaned Agreement Form (Pupils)

Pupil Loaned Agreement Form

Appendix 6: IT Technician online safety incident logs

Discovery Trust IT Technician Online Safety Monitoring Logs