REPTON
PREP

# Online Safety Policy

Last Reviewed: Michaelmas 2023
Next Review: Michaelmas 2024



Milton · Derbyshire · DE65 6EJ
Charity number: 1093165 Company number: 04390208

# Contents

This policy is relevant to all staff and applies to all pupils from Early Years to Year 8. It should be read in conjunction with the following:

- Behaviour Management Policy
- Anti Bullying Policy
- Boarding Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct

## Key Contacts

| Repton Prep School | |
|---|---|
| Mrs Vicky Harding<br>Head | vharding@repton.org.uk<br>01283 707100 |
| Mr Mat Shepherd<br>Digital Development Manager<br>(responsible for IT Network and Systems)<br><br>IT network and systems are managed by European Electronique (EE) | mshepherd@repton.org.uk<br>01283 559313<br><br>servicedesk@repton.org.uk<br>07970 779041 |
| Mr Stuart Elks<br>Designated Safeguarding Lead (DSL) and Online Safety Coordinator | selks@repton.org.uk<br>01283 707111 |
| Ms Kellee Cavill<br>Deputy DSL | kcavill@repton.org.uk<br>01283 707118 |
| Liaison Governor for Child Protection, Ms Sally Wan (Nominated Safeguarding Governor) | *Contact without divulging any details is available via Rachel Mair, the Clerk to the Governors, calling 01283 559272 or using rmair@repton.org.uk* |

External:

| | |
|---|---|
| **Derbyshire Childrens Services:** | |
| Derby & Derbyshire Childrens Safeguarding Partnership (DDSCP) – Starting Point (for referrals) | 01629 533390 /<br>https://www.ddscp.org.uk/ |
| Local Authority Designated Officer (LADO) – Mr Miles Dent – for allegations against staff | 01629 531940 /<br>miles.dent@derbyshire.gov.uk |
| Child Protection Manager for Schools/Educational Settings, Derbyshire County Council – Ann Holmwood | ann.holmwood@derbyshire.gov.uk<br>07795 316055 |
| **The Police:** | |
| Police (non-emergencies) / Police emergencies | 101 / 999<br>Central Referral Unit: Butterley Hall, https:www.ceop.police.uk/ Derbyshire DE5 3RS 0300 122 8719 |
| CEOP (Child Exploitation and Online Protection) | https://www.ceop.police.uk/Safety-Centre/ |
| **Extremism:** | |
| PREVENT Derbyshire County Council – Mr Seamus Carroll | Seamus.carroll@derbyshire.gov.uk01629 538494 / 07771 980107 |

| | |
|---|---|
| PREVENT Regional Coordinator East Midlands providing advice for schools and childminders – Mr Sam Slack | sam.slack@education.gov.uk |
| Derbyshire Police PREVENT Team | 0300 1228694 |
| Anti-terrorism helpline | 0800 789321 |
| **Other:** | |
| NSPCC Inform | 0808 800 5000 / help@nspcc.org.uk / https://www.nspcc.org.uk/keeping-children-safe/reporting-abuse/ |
| NSPCC Whistleblowing Helpline | 0800 0280285 / help@nspcc.org.uk |
| Kidscape (Anti-bullying helpline for parents) | 0845 1205204 |

# 1 Information on internet technology

## 1.1 Introduction

The educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. Repton Prep needs to be able to teach children how to keep themselves safe whilst on-line.

This policy provides Repton Prep with guidance on managing online safety so that these aims can be achieved and to support staff to recognise the risks and take action to help children use the internet safely and responsibly.

## 1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

### 1.1.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children.

There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

### 1.1.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child or for child-on-child abuse. More details on this can be found in section 4.5 of this policy.

### 1.1.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents.

They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

### 1.1.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- online bullying and child-on-child abuse (see section 4.5 for further details)
- use of mobile devices for the purposes of sexual harassment such as the consensual and non-consensual taking and distributing of inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

# 2 Repton Prep online safety strategies

## 2.1 Whole school approach

Computing is a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Repton Prep will consider the following in order to ensure a holistic approach to online safety:

- Staff should be aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and should be aware of the use of technology in child-on-child abuse.
- When developing new policies, Repton Prep will ensure online safety and the impact of technology is considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.
- Repton Prep will ensure that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff should receive suitable training

around online safety and similar messages should be taught to pupils.

- Staff should be aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with pupils, and the school must ensure there are clear policies available to staff on expectations for online behaviour.
- There should be a clear link between the Online Safety policy and the Behaviour Management policy that sets out expected standards for pupil's online behaviour and expected sanctions for breaches.
- The Online Safety policy should be reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

Repton Prep will refer to the following DfE non-statutory guidance on teaching online safety: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE:
https://www.gov.uk/government/publications/relationships-education- relationships-and-sex-education-rse-and-health-education

### 2.2 Purpose and description

Repton Prep will have an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

In particular schools must ensure the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (Repton Prep use Securly)
- A culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of on-line behaviour.
- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

### 2.3 Roles and responsibilities

#### 2.3.1 Head's role

The Head has ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data

- ensuring that online safety issues are given a high profile within the school community
- linking with governors and parents and carers to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

### 2.3.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the Head in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors should liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

### 2.3.3 Online Safety Coordinator's role

All schools should have a designated Online Safety Coordinator who is responsible for co-ordinating online safety policies on behalf of the school. Ideally, the officer should be a senior member of the management team.

Given the issues associated with online safety, it is appropriate for the DSL to be the school's Online Safety Coordinator.

The Online Safety Coordinator should have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's Online Safety policy
- ensure that staff and pupils are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's network manager, the Head and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems and that the school has appropriate

filtering and monitoring systems

- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- ensure that all staff and pupils have read and understood the acceptable use policy (AUP)
- report annually to the board of governors on the implementation of the school's online safety strategy
- maintain a log of internet related incidents and co-ordinate any investigation into breaches

#### 2.3.4 Network manager's role

Their role is:

- the maintenance and monitoring of the school internet system including anti-virus and filtering and monitoring systems
- carrying out monitoring and audits of networks and reporting breaches to the Online Safety Coordinator
- supporting any subsequent investigation into breaches and preserving any evidence.

#### 2.3.5 Role of all Repton Prep staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's Online Safety and Acceptable Use policies and procedures
- communicating the school's Online Safety and Acceptable Use policies to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the Online Safety Coordinator
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the Online Safety Coordinator
- teaching the online safety and digital literacy elements of the new curriculum.

#### 2.3.6 Designated Safeguarding Leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the DSL who will decide whether or not a referral should be made to DDSCP or the Police.

### 2.4 Pupils with special educational needs and disabilities (SEND)

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. Repton

Prep will have a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

The Head of Learning Enhancement is responsible for providing extra support for these pupils and should:

- link with the Online Safety Coordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- where necessary, liaise with the Online Safety Coordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- ensure that the school's Online Safety policy is adapted to suit the needs of pupils with SEND
- be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences
- liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.

### 2.5 Working with parents and carers

It is essential that Repton Prep involves parents and carers in the development and implementation of online safety strategies and policies; most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

Repton Prep will offer online safety training opportunities and resources to parents in order to provide them with information to help them keep their child safe online.

The Head, board of governors and the Online Safety Coordinator should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Parents should be provided with information on computing and the school's Online Safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Parents should also be informed that they can contact the school's Online Safety Coordinator if they have any concerns about their child's use of technology.

Where remote online learning is being used, parents should be made aware of what

arrangements have been made, which websites children will be accessing and any member of staff they will be interacting with online.

# 3 Online safety policies

## 3.1 Accessing and monitoring the system

- Access to the school internet system should be via individual logins and passwords for staff and pupils wherever possible. Visitors should have permission from the Head or Online Safety Coordinator to access the system and be given a separate guest login.
- The Online Safety Coordinator should keep a record of all logins used within the school for the purposes of monitoring and auditing internet activity.
- Staff should be required to change their password every 6 months.
- The Online Safety Coordinator and teaching staff should carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

## 3.2 Privacy and Security

3.2.1 Routine Logging and Monitoring: Certain central service and network activities from workstations connected to the network are routinely logged and monitored. These activities include: use of passwords and accounts accessed, time and duration of network activity, access to Web pages, access to software, volume of data storage and transfers, volume of e-mail access from outside school.

3.2.2 Detailed Session Logging: In cases of suspected violations of Repton Prep policies, especially unauthorised access to computing systems, the system administrator concerned may authorise detailed session logging. This may involve a complete keystroke log of an entire session. In addition, the system administrator of the facility concerned may authorise limited searching of user files to gather evidence on a suspected violation.

3.2.3 Responsibility for Data Security: Software and physical limitations, computer viruses, and third-party intrusions can compromise security of data storage and communications. Repton Prep takes reasonable precautions to minimise risk. The IT support team use various technologies to maintain backups of school data but is not obligated to maintain backups of any file for any particular length of time. Users must protect and back up critical data. Individual users and departments should develop policies and practices to ensure regular backups of data and implement steps to ensure that all critical data is compatible with all current generations of computing equipment, storage media, and media readers.

3.2.4 Restriction of Access to Sensitive Data: All Repton Prep departments should implement policies to ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords restricting access to information should be changed on a regular basis and systems should be developed and implemented to assure password records are regularly updated by appropriate supervisors.

3.2.5 Right to Examine Computers and Equipment: Computers and equipment owned by Repton Prep or connected to the Repton Prep network may be examined to detect illegal software and to evaluate the security of the network.

### 3.3 Confidentiality and data protection

- Repton Prep will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely, and password protected with access given only to staff members on a "need to know" basis.
- The school will endeavour to password protect sensitive pupil data that is being sent to other schools or organisations, for example future schools. Any breaches of data security should be reported to the Head and Data Protection Officer immediately.
- Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.

### 3.4 Acceptable use policies

- All internet users within the school will be expected to adhere to an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the Repton Prep online safety rules regarding their internet use.
- For pupils in EYFS to Year 4, acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet in school (see Appendix 1).
- For pupils in Years 5-8) both the pupil and their parents will sign the acceptable use policy, and use of the internet in school is dependent on signing this agreement (see Appendix 2).
- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see Appendix 3).
- The school's Online Safety Coordinator will keep a copy of all signed acceptable use agreements.

### 3.5 Teaching online safety

#### 3.5.1 Responsibility

One of the key features of the Repton Prep's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the Head and the Online Safety Coordinator, in conjunction with the Head of ICT, but all staff should play a role in delivering online safety messages.
- The Online Safety Coordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.
- The Head of ICT and classroom teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Repton Prep is required to teach about online bullying as part of statutory Relationships Education (primary), Relationships and Sex Education (secondary) and health education (all schools).
- PSHE lessons provide an ideal for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills for example pupils with SEND.
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to both at school and during school trips and off-site activities.

### 3.5.2 Content

Pupils should be taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies;
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems;
- are responsible, competent, confident and creative users of information and communication technology.

**Primary pupils (EYFS to Year 6)** should be taught all elements of online safety included in Statutory Relationships Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help
- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

**Statutory Health Education** should include:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.

- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- where and how to report concerns and get support with issues online.

**Secondary pupils (Years 7 and 8)** should be taught all elements of online safety included in statutory Relationships and Sex Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.
- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- what to do and where to get support to report material or manage issues online.
- the impact of viewing harmful content.
- that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- how information and data is generated, collected, shared and used online.

**Statutory Health Education** should include:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

## 3.6 Staff training and conduct

### 3.6.1 Training

- All Repton Prep staff and governors should receive training with regard to IT systems and online safety as part of their induction and this should include a meeting with the Online Safety Coordinator and the network manager.
- Staff should also attend specific training on online safety available from the DDSCP so that they are aware of the risks and actions to take to keep pupils safe online. The Head and SMT should ensure that regular update training is included at staff INSET in order to ensure all staff can keep up with new developments in technology and any emerging safety issues.

### 3.6.2 IT and safe teaching practice

Repton Prep staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.
- Staff should always use Repton Prep equipment and only store images on the school computer system
- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.
- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.
- Staff should be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.
- Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the Repton Prep or their profession into disrepute.
- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.
- Where staff need to communicate with pupils regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.
- When making contact with parents or pupils by telephone, staff should only use Repton Prep equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.
- When making contact with parents or pupils by email, staff should always use their Repton Prep email address or account. Personal email addresses and accounts should never be used.
- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.
- Where staff are using mobile equipment such as laptops or tablets provided by Repton Prep, they should ensure that the equipment is kept safe and secure at all times.

### 3.6.3 Exit strategy

- When staff leave, their line manager should liaise with the network manager to ensure that any Repton Prep equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from Repton School/Repton Prep's IT system.

## 3.7 Safe use of technology

### 3.7.1 Internet and search engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.
- Primary school aged children should be supervised at all times when using the internet. Although supervision of secondary school aged pupils will be more flexible, teachers should remain vigilant at all times during lessons.
- Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the Online Safety Coordinator, who will liaise with the IT service provider for temporary access.

### 3.7.2 Evaluating and using internet content

- Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

### 3.7.3 Safe use of applications

**School email systems** should be hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally.

**Social networking sites** such as Facebook, Instagram and Twitter/X allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

**Online communities and forums** are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

**Chat rooms** are internet sites where users can join in "conversations" on-line; **instant messaging** allows instant communications between two people on-line. In most cases, pupils will use these at home although school internet systems do host these applications.

**Gaming-based sites** allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently, such sites should not be accessible via school internet systems

## Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the Repton Prep internet system is forbidden and is usually blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.
- If schools identify a clear educational use for social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.
- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the Online Safety Coordinator who will liaise with the learning platform provider.
- Apart from the Head, individual email addresses for staff or pupils should not be published on the Repton Prep website.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.
- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.
- Pupils should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's Anti-Bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.
- Users should be aware that use of the Repton Prep internet system is for the purposes of education or school business only, and its use may be monitored.
- In order to teach pupils to stay safe online outside of school, they should be advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    - to only use moderated chat rooms that require registration and are specifically for their age group;
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
    - not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents

or carers know so that appropriate action can be taken.

### 3.7.4 Video calling and remote learning

Video calling or live streaming enables users to communicate face-to-face via the internet using web cameras. When carrying remote learning, the following should be taken into account:

- only using Repton Prep registered accounts rather than personal accounts
- recording remote learning for safeguarding purposes
- the security of the video link
- checking settings regularly to ensure teachers have full control of the meeting i.e. Who can start, join or chat in the stream
- paying attention to background settings to prevent breach of privacy
- training for teachers to use the new technology
- a system for teachers to log any remote learning contacts and issues.

### 3.7.5 School website

- Content should not be uploaded onto the Repton Prep website unless it has been authorised by the Head and Marketing Department, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.
- The designated person(s) to have responsibility for uploading materials onto the website is the Repton Marketing Department.
- To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No personal contact details for staff or pupils should be contained on the website.
- Children's full names should never be published on the website.
- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

### 3.7.6 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.
- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.
- Children's full names should never be published where their photograph or video is being used.
- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.
- Images should be securely stored only on the Repton Prep's computer system and all other copies deleted.
- Stored images should not be labelled with the child's name.
- Staff are **not** permitted to take photographs of pupils in class, at any school events or on a school trip using a personal device. There is a separate policy that outlines these instructions for EYFS. No photos should be shared on any social media sites or apps, including WhatsApp. Photographs or video camera footage should only be taken on school owned devices and transferred to the school system. Please contact the Senior Deputy Head and DSL regarding the use of school owned devices and for any

safeguarding implications. Repton Prep will endeavour to inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

### 3.7.7 Pupils own mobile devices

- At Repton Prep we endeavour to ensure that all pupils are able to gain access to the support and resources that will allow them to fulfil their academic potential and this may include the use of portable electronic devices (PEDs). It is not our intention to ban PEDs in school, but to effectively manage their use and for pupils to take responsibility for their safety and appropriate use. If they are required for academic purposes, PEDs will be provided by the school.
- Due to the multi-functionality of PEDs, this policy differentiates between functions and not devices. The word 'portable' refers to hand-held devices up to and including tablets such as the iPad in size, but not laptop or netbook computers.
- Parents and pupils should note that, due to their high monetary value, Repton Prep does not encourage the presence of PEDs on its premises, and that the School is not liable for any loss or damage to these devices on the Repton Prep site, at any time. All valuables, including PEDs are brought onto the site at the owner's discretion and risk.
- No pupils in Pre-Prep should have PEDs in school unless it is specifically recommended by the Head of Learning Enhancement (or in the case of boarders, the Head of Boarding). If this is the case, a parent/pupil contract should be completed and the rest of this policy then applies.
- Pupils in Prep are only permitted to have a PED in school once the parent/pupil contract has been received, and permission has been granted by the Head of Learning Enhancement (or in the case of boarders, the Head of Boarding). A list of these pupils, and the device that they have been given permission to use, will be made available to all teaching staff.
- All PEDs are the responsibility of the pupil/parent who should ensure that appropriate insurance and safeguards are in place, to include accidental damage. The Repton Prep school's insurance does not cover PED's belonging to pupils.
- There may be occasions when pupils are permitted to take PEDs on long journeys/residential trips. The trip leader should give consideration as to the safety of these devices at the destination as a part of the trip planning.
- All pre-downloaded material on the PED must be age appropriate.
- Whilst in school, responsibility for PEDs lies solely with the pupil.
- PEDs in school are for personal use only and must not be loaned or shared.

- Pupils must seek permission from the member of staff supervising them before attempting to use a PED. Permission must not be assumed. PEDs must only be used for school-related activities under the supervision of a member of staff. The permission is given on an individual basis and only lasts until the end of that lesson/session. If a teacher gives permission for a device to be used for one purpose, then the pupil may not assume permission for other purposes: e.g., a tablet which is being used to read a book may not then be used as a word processor unless the teacher specifically gives their permission.
- Pupils must not use PED's to photograph or record another person whilst at school.
- PEDs must not be taken into changing rooms/toilets etc.
- PEDs must not be charged in school, except in the case of boarders who may charge them in the boarding houses.
- Any pupil in breach of any part of this policy will have their device confiscated and the privilege to bring these devices into school may be withdrawn. In addition, they may be disciplined according to the school's policy.
- Confiscated devices will be placed away safely in the School Office and may be collected by parents or house parents.

Examples of functions on PEDs that may legitimately be used by pupils:

**Mobile Phones**

- Day pupils are not permitted to have, or use, mobile phones at school
- Boarders are permitted to have mobile phones outside of the normal school day, in the evening and at weekends. Access will always be managed and supervised by a member of the boarding team and in accordance with boarding policy.
- If day pupils are required to bring a mobile phone to school (for instance for use during the journey to and from school), they should be left in the care of the School Office for the duration of the school day.
- No pupils are permitted to take Mobile phones on any school trips – both day and residential.
- Boarders must only access the internet using the Repton Prep IT network as they could otherwise obtain unlimited and unrestricted access to the internet via mobile phone 3G/4G/5G networks. Such access would lead some children, whilst at school, to potentially sexually harass, bully and control others via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. All staff should be alert to this safeguarding threat and report any concerns to the DSL immediately.

**Reading**

- Pupils are permitted to use PEDs to read pre-downloaded eBooks
- All pre-downloaded eBooks should be age appropriate.
- Staff should monitor for use of appropriate reading material.

**Translation**

- PEDs may be used by some pupils as an electronic dictionary/translator.

**Music**

- Many PEDs have the facility for music to be played. Playing music on a PED is not permitted in school and will only be allowed when on long journeys/residential trips or in the boarding house and when expressly permitted by the member of staff in charge.

**Medical**

- Repton Prep recognises that PEDs are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs.
- Where a pupil needs to use a mobile device for such purposes – for instance monitoring the operation of a pump regulating the blood sugar levels of a pupil who is diabetic – the pupil's parents or carers should arrange a meeting with the School Nurse, Head of Learning Enhancement, Deputy Head Pastoral and Boarding, Deputy Head Pre-Prep or Senior Deputy Head (as appropriate). At this meeting it will be agreed as to how the school can appropriately support the use of mobile technology for the pupil's needs. The appropriate member of staff co-ordinating the school's support of the pupil in question will inform their teachers and other relevant members of staff about how the pupil will use the device at school.

**Games**

- Many PEDs have the facility for games to be played. Playing these games is not permitted in school and will only be allowed when on long journeys/residential trips or in the boarding house and when expressly permitted by the member of staff in charge.

# 4 Responding to incidents

## 4.1 Policy statement

- All significant or complex incidents and complaints relating to online safety and unacceptable internet use will be reported to the Online Safety Coordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the Online Safety Coordinator on the online safety incident report form (Appendix 4).
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Head for action under staff code of conduct policies for low level incidents or consideration given to contacting the LADO under the DDSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the Head should be reported to the Chair of Governors.
- The school's Online Safety Coordinator will keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and use these to update the online safety policy.
- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the DSL, who will make a decision as to

whether or not to refer the matter to the police and/or the LADO in conjunction with the Head.

- Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Repton Prep cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

### 4.2 Reporting Incidents

- Repton Prep uses the online reporting tool, Whisper. This allows pupils and parents to raise any concerns via SMS message or via the Whisper website and, should they wish, this can be done anonymously. Whisper can be used to raise concerns relating to safeguarding issues such as friendship issues, mental health concerns, concerns for wellbeing or online issues. This is a two-way communication tool (School will not have access to any contact information), in order that School can provide the relevant and appropriate advice and support. Whisper is monitored by the DSL and DDSL.

- Repton Prep's DSL and DDSL receive notifications from Securly regarding any online searches that are deemed inappropriate/a risk. Each alert is investigated as soon as is practicable. All details and results of the investigation/subsequent action are logged on Repton Prep's Filtering and Monitoring log.

### 4.3 Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.
- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.
- The incident should be reported to the Online Safety Coordinator and details of the website address and URL provided.
- The Online Safety Coordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

### 4.4 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the Acceptable Use Policy and subject to appropriate sanctions (see section 5).
- The incident should be reported to the Online Safety Coordinator and details of the website address and URL recorded.
- The Online Safety Coordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.
- The pupil's parents should be notified of the incident and what action will be taken.

### 4.5 Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the Head and the Online Safety Coordinator immediately. If the misconduct involves the Head or a Governor, the matter should be reported to the Chair of Governors.
- The Online Safety Coordinator will notify the network manager so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.
- The Online Safety Coordinator will arrange with the network manager or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established, the Head will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.
- If the materials viewed are illegal in nature, the Head or Chair of Governors should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.

### 4.6 Online bullying

#### 4.6.1 Definition and description

- Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.
- Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.
- Bullying may take the form of:
    - rude, abusive or threatening messages via email or text
    - posting insulting, derogatory or defamatory statements on blogs or social networking sites
    - setting up websites that specifically target the victim
    - making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, sexting/"happy slapping").

- Online bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

#### 4.6.2 Dealing with incidents

- The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school. All incidents should be dealt with under the schools' behaviour policies and the child-on-child abuse guidance.
- Repton Prep Anti-Bullying, Behaviour Management Policies and Acceptable Use Policies cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of online bullying should be reported to the Online Safety Coordinator who will record the incident on the incident report form and ensure that the incident is dealt with in line with the Repton Prep's Anti-Bullying Policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.
- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.
- As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.
- Pupils should be taught:
    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to send or post inappropriate images of themselves
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.
- Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions.

### 4.6.3 Action by service providers

- All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.
- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The pupil should also consider their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The pupil should also consider changing email address.
- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

#### 4.6.4 Online bullying of Repton Prep staff

- The Head is aware that school staff may become victims of online bullying by pupils and/or their parents. Because of the duty of care owed to staff, the Head will ensure that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents.
- Incidents of online bullying involving school staff will be recorded and monitored by the Online Safety Coordinator in the same manner as incidents involving pupils.
- Staff should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.
- Personal contact details for staff will not be posted on the Repton Prep website or in any other school publication.
- Staff should follow the advice above on online bullying of pupils and not reply to messages but report the incident to the Head immediately.
- Where the bullying is being carried out by parents, the Head should contact the parent to discuss the issue. A home/school agreement with the parent may be used to ensure responsible use.

### 4.7 Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute sexual harassment or online bullying and because of the nature of online activities this can lead to more widespread harm and repeat victimisation.

*Keeping Children Safe in Education 2023* places a duty on schools to respond to any incidents of online sexual harassment such as:

- consensual and non-consensual sharing of nude and semi-nude images
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats
- coercing others into sharing images or performing acts online that they are not comfortable with.

For further details on what actions need to be taken in response to online sexual harassment, Repton Prep School will refer to the following DfE guidance:
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

Repton Prep will make pupils aware that producing and distributing sexual images to peers via the internet or mobile devices may be illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised.

Repton Prep staff will refer to the following DfE guidance for responding to incidents: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

### 4.8 Risk from inappropriate contacts with adults

- Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.
- School staff should also be aware of pupils being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.
- All concerns around inappropriate contacts should be reported to the Online Safety Coordinator and the DSL.
- The DSL should discuss the matter with the referring teacher and, where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to the LADO and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
- The DSL can seek advice on possible courses of action from Derby & Derbyshire Childrens Safeguarding Partnership (DDSCP).
- Teachers will advise the pupil on how to terminate the contact and change contact details where necessary to ensure no further contact.
- The DSL and the Online Safety Coordinator should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school IT equipment or networks, the Online Safety Coordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

### 4.9 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Derbyshire Constabulary Prevent Team, a multi-agency forum that identifies young people who

are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against Repton Prep policies.
- The school should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents should be dealt with as a breach of the Acceptable Use Policies and the school's Behaviour and staff disciplinary procedures should be used as appropriate.
- The Online Safety Coordinator and the DSL should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, Repton Prep will refer the young person to the DDSCP.

### 4.10 Risk from sites advocating suicide, self-harm and anorexia

- Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.
- Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.
- Repton Prep will ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.
- Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

# 5 Sanctions for misuse of school IT

## 5.1 Sanctions for pupils

### 5.1.1 Category A infringements

These are low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions will include:

- referral to the Form Tutor and the Online Safety Coordinator.
- completion of a Written Reflection (or Ref) in line with Phase 2 of the Sanctions Hierarchy and Process in the Behaviour Management Policy

### 5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- using/carrying an unsanctioned portable electronic device, such as a mobile phone
- online bullying (first offence)
- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions will include:

- referral to the Form Tutor, the Online Safety Coordinator and the Head of Year (and the Head in some cases)
- completion of an Order Mark in line with Phase 3 (or in more serious cases a Head's Detention in line with Phase 4) of the Sanctions Hierarchy and Process in the Behaviour Management Policy
- loss of internet access for a period of time
- contact with parents.

### 5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- continued online bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions will include:

- referral to the Form Tutor, the Online Safety Coordinator, the Head of Year and the Head.
- completion of a Head's Detention in line with Phase 4 or a temporary suspension or permanent exclusion in line with Phase 5 of the Sanctions Hierarchy and Process in the Behaviour Management Policy
- loss of access to the internet for a period of time
- contact with parents

### 5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme online bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act

Sanctions will include:

- referral to the Online Safety Coordinator, the Head of Year and the Head.
- temporary suspension or permanent exclusion in line with Phase 5 of the Sanctions Hierarchy and Process in the Behaviour Management Policy
- removal of equipment
- possible referral to community police officer

## 5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the Repton Prep Staff Code of Conduct.

### 5.2.1 Category A infringements

These are minor breaches of the school's Acceptable Use policy which amount to misconduct and will be dealt with internally by the Head as a low-level incident in line with the Staff Code of Conduct

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (e.g. removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter/X that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanction may include referral to the Head/HR who will issue a warning.

### 5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or LADO.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act

- bringing the Repton Prep/Repton School name into disrepute.

Possible sanctions include:

- referral to the Head and Director of HR
- removal of equipment
- referral to the police
- referral to the LADO
- suspension pending investigation
- disciplinary action in line with school policies

Appendix 1: **Acceptable Use Policy for pupils in EYFS to Year 4**

| **Pupil's Name:** |
| --- |
| **Form:** |

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

**I will:**
• keep my password a secret
• only open pages which my teacher has said are okay
• tell my teacher if anything makes me feel scared or uncomfortable
• make sure all the messages I send are polite
• tell my teacher if I get a nasty message
• not reply to any nasty message which makes me feel upset or uncomfortable
• not give my mobile number, home number or address to anyone who is not a real friend
• only email people I know or if my teacher agrees
• only use my Repton Prep email address
• talk to my teacher before using anything on the internet
• not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
• not load photographs of myself onto the computer
• never agree to meet a stranger.

**Parents (please tick)**
□ I have read the above Repton Prep rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.

□ I agree that my child's work can be published on the Repton Prep website, in school publications and on school's social media for legitimate marketing purposes.

Signed:

Date:

Appendix 2: **Acceptable Use Policy for pupils in Years 5 to 8**

*The pupil element of this form is completed as an online form each academic year in the first computing lesson of the new academic year. Pupils joining the school at other times in the academic year are prompted to complete it when they access the school IT system for the first time.*

**General statement**
The computers are provided and maintained for the benefit of all children, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or around school. The Repton Prep Code applies. Remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

☐ I agree to use the Repton Prep IT network

**Equipment**
- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not open files brought in on removable media (such as floppy disks, CDs, USB drives etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Do not eat or drink near computer equipment.

☐ I have read this. I agree and understand.

**Security and privacy**
- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, any details about school, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and web accounts will be treated like school desks. Staff may review files and communications to ensure that users are using the system responsibly.

☐ I have read this. I agree and understand.

**Using the Internet**
- The Internet should only be used for study or for school authorised/supervised activities.
- Do not use the Internet or online accounts to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which

could be used by others to benefit their studies.
- Never arrange to meet anyone via the Internet. People you contact online are not always who they seem.

☐ I have read this. I agree and understand.

**Email and messaging**
- Be polite and appreciate that other users might have different views from your own.
- The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content.
- Always report such messages to a member of staff.

☐ I have read this. I agree and understand.

**Enforcement**
This document is to be read carefully by all pupils. If any child disobeys these provisions, access to the Internet will be denied and sanctions may be issued in line with the Online Safety Policy.

☐ I agree to use the IT network safely and responsibly.

*The details of this AUP are also sent to parents annually.*

**Parents (please tick)**
□ I have read the above Repton Prep rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.

□ I agree that my child's work can be published on the Repton Prep website, in school publications and on school's social media for legitimate marketing purposes.

Signed:

Date:

Appendix 3: **Acceptable Use Policy for Staff and Governors**

# IT Acceptable Use Policy

## Purpose

a) This policy is designed to protect pupils, staff, and the school. It is in accordance with the UK Computer Misuse Act, (1990), and any subsequent revision, and may be subject to change without notice.
b) This policy covers all Pupils, Staff, Teachers, Employees, Contractors, Volunteers, Interns, Casual workers, temporary and agency workers, and anyone who has access to our IT and communication systems, on any part of the school campus or via any means of remote access.
c) Our IT and communications systems include fixed devices, mobile devices and telephones and this policy applies whether or not the device or system in question is owned by the school.
d) Our IT and communications systems are intended to promote effective learning, communication, administration and working practices throughout our schools. This policy outlines the rights and obligations of Users, the standards that must be observed when using these systems, the circumstances in which we will monitor system use, and the action we will take in respect of breaches of these standards.
e) Misuse of IT and communications systems can damage our educational outcomes, pupil and staff wellbeing, our school, and our reputation. This policy is designed to ensure a clear, defined balance between the need for open communication and the protection of the school's pupils, staff, assets, and reputation.
f) The school takes compliance with this policy very seriously. Failure to comply could put pupils, staff, and the school at risk. Failure to comply with any requirement of this policy may result in disciplinary action up to and including dismissal (staff) or exclusion (pupils), and criminal proceedings.

## Security and Passwords

a) You are personally responsible for the security of the equipment allocated to or used by you. You must not allow it to be used by anyone other than in accordance with this policy.
b) You should always lock or log-off from any electronic device when not in use, to prevent unauthorised access.
c) You should not attempt to bypass security systems / Internet filtering on school networks by any means.
d) IT and communication devices should always be kept secure. If you misplace or have any IT or communications device stolen, you must notify the Digital Development Manager immediately.
e) You will be held personally responsible for any activity carried out using your user credentials for any school system, which must therefore not be shared with anyone except for the IT Support Team (European Electronique), for the purposes of troubleshooting.
f) Additional passwords and encryption should be used where appropriate to secure access to sensitive / confidential information stored on electronic devices.
g) You should not attempt to gain or use any password other than your own.
h) The school reserves the right to install / uninstall software on user devices at any time, as required by the Safeguarding team, compliance function, or HR department, without prior notice.

## Internet / Network Access

a) All internet traffic via school networks / Wi-Fi is filtered and monitored to prevent access to content deemed inappropriate.
b) Any Internet connection outside the school network presents a higher risk to your personal information and may allow access to content not normally permitted in school.
c) Particular care should be taken to ensure pupil mobile devices (phones, tablets, laptops) with mobile data capability have appropriate controls set by parents / guardians.
d) School-owned devices must only connect to the Internet using school networks and must never be connected / tethered to mobile devices with data capabilities without the approval of the Headmaster (Senior), Head (Prep) or Designated Safeguarding Leads.
e) A separate network is provided for personal devices (mobile phones, tablets, laptops) which is subject to the same filtering / monitoring rules.
f) Users must not attempt to connect any networking device to the school network (network hubs / switches / wireless access points / wireless routers / wireless extenders / routers etc).
g) Users will not use the school Network to access, distribute or make available inappropriate material. For the avoidance of doubt, this includes any material that may be deemed illegal, offensive, discriminatory, in bad taste, immoral or in breach of copyright, in any format.

h) Users will not access school networks or the Internet for fraud, financial gain, software piracy, copyright infringement or any other malicious act.
i) Users will not make use of any type of file sharing technology for the purposes of sharing non-school related content.
j) Users must not add / remove / modify any hardware or software on school computers
k) Any additional software required in the pursuance of your studies / work must be requested from the IT Support Team (European Electronique), who will obtain academic / administrative guidance before any installations are undertaken.
l) Social Media is not deemed appropriate for use in school and is blocked from the main school network – please check with the Safeguarding team if you have a specific requirement. Certain sites may be permitted for specific use.

## Electronic communication (email, MS Teams)

a) Users will not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate emails or messages via any means of electronic communication. If you feel that you are being, or have been, harassed or bullied, or if you are offended by material received from a peer / colleague, you should inform your Housemaster / Housemistress or the Safeguarding team (pupils) or the HR department (staff).
b) Users must not use electronic communication tools for the mass distribution of unsolicited messages and must not create or distribute materials which are designed or likely to cause annoyance, inconvenience, or needless anxiety.
c) Users must not forward messages to other people without first obtaining the original sender's permission.
d) Users must remember that any undertakings given by e-mail may be legally binding.

## Legal Requirements

a) Users will accept full responsibility for the legality of all software installed on their devices.
b) Users will observe and adhere to the law on copyright and the General Data Protection Regulation (GDPR) at all times.

## Enforcement, monitoring and privacy

a) Users agree to all monitoring and filtering by School systems while their devices are connected to the school network.
b) Where an alleged breach of this policy has occurred, or is reasonably suspected to have occurred, SMT members, the Digital Development Manager and the IT Support Team (European Electronique) are legally permitted to inspect electronic devices. This may involve confiscation of the device and inspection of the contents of a user's files or email messages, as defined in the Department for Education "Searching, screening and Confiscation (2018)

guidance", which can be found here.

## School Data

a) By following standard practice and ensuring any work is always created in and saved to the systems provided by the school (OneDrive, SharePoint, Outlook, etc) backups of work will be created automatically. Saving any data locally to a PC / laptop / Surface / USB drive / mobile phone or other device is strongly discouraged as this provides NO backup of your data and it is unlikely that you will be able to recover any work saved locally in the event of device failure.
b) Staff are reminded that school data should not be saved to any location outside school systems (Dropbox, iCloud, etc).

## Personal Data

a) Personal data should always be backed up externally from school systems to an individual's personal choice of location (USB stick, external hard drive, Dropbox, iCloud, etc). The school does not back up personal files or any data not stored on school systems (OneDrive, Teams, etc). In the event of loss of this type of file, the school is under no obligation to attempt to retrieve / restore these files.

## General Notes

a) Boarding pupils may only use electronic devices after bedtime with express permission to do so from the Housemaster / Housemistress.
b) Any comments on websites concerning the school or individuals representing the school should always be responsible, thoughtful, considerate and bring credit to the individual and the school.

M. Shepherd - Digital Development Manager
October 2023

Appendix 4: **Online safety incident report form**

**Details of incident**

| |
|---|
| **Date** incident occurred:<br>**Time** incident occurred: |

| |
|---|
| **Name of person reporting incident:**<br>If not reported, how was the incident identified? |

| |
|---|
| **Where did the incident occur?**<br>□ In school setting<br>□ Outside school setting |

| |
|---|
| **Who was involved in the incident?**<br>□ child/young person<br>□ staff member<br>□ other (please specify) |

| |
|---|
| **Type of incident:**<br>□ bullying or harassment (online bullying)<br>□ deliberately bypassing security or access<br>□ hacking or virus propagation<br>□ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material<br>□ terrorist material<br>□ online grooming<br>□ online radicalisation<br>□ child abuse images<br>□ on-line gambling<br>□ soft core pornographic material<br>□ illegal hard core pornographic material<br>□ other (please specify) |

| |
|---|
| **Description of incident:** |

**Nature of incident**

□ **Deliberate access**
Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ online bullying □ breach of AUP

□ **Accidental access**
Did the incident involve material being;
□ created □ viewed □ printed □ shown to others □ transmitted to others □ distributed

**Action taken**
**Staff**
□ incident reported to Head/SMT
□ advice sought from LADO
□ referral made to LADO
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended
**Please detail any specific action taken (i.e. removal of equipment):**

**Child/young person**
□ incident reported to Head/SMT
□ advice sought from DDSCP
□ referral made to DDSCP
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT Network Manager
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ online safety policy to be reviewed/amended

**Outcome of incident/investigation**