Data protection Act UK

UNLOCKING POTENTIAL

LEVELLING THE SOCIAL AND ACADEMIC ARENA

DIGITAL SAFETY POLICY

(incorporating Online Safety, ICT & Acceptable Internet Use, Mobile Phones and Remote Learning)

Mission Statement

The Levels School exists to provide a nurturing environment in which students with specific learning difficulties and co-occurring diagnoses can develop their self-esteem and aspire to be independent young adults who value the rights, responsibilities and rules that exist to promote and support their future welfare. Our approach toward establishing this ideology is predicated on trauma-informed practice and an obligation to develop the social skills required to build their future aspirational communities. We exist to help them find their level.

This policy covers all premises known as The Levels School.

Date of policy	September 2026
Next review date	September 2027
Frequency of policy review (annually, every two years)	Annual
Policy owner	Ben Bridger and Caroline Cook
Published policy	Yes ☒ No ☐

List of connected policies	Safeguarding, Anti-Bullying policy, Relational Policy, Exclusion policy, Staff Code of Conduct, Complaints, Data protection policies and procedures
Approved by	Approved by Governors

The Board of Governors acknowledge their responsibility to ensure that this policy is effective and follows regulatory requirements. Governors undertake a review to satisfy themselves that the implementation of this policy is effective.

The Board of Governors ensures the establishment of familiarity with and the effective operation through monitoring, of school policies, approving those requiring GB sign-off in line with a regular cycle of school policy reviews. This occurs through a cycle of governor committee meetings and full board meetings.

Contents

Mission Statement 1
Contents 3
Contacts List 5
Rationale 6
Relevant Legislation and Guidance 7
Definitions 7
Roles and responsibilities 8
The governing board 8
The Head teacher 8
The ICT & Network Manager 8
The Designated Safeguarding Lead (DSL) 9
The ICT Development and Strategy manager 9
All staff and volunteers 10
Parents 10
Students 11
Visitors and members of the community 11
ICT Development 11
Part 1 – Acceptable Use 13
Unacceptable use of the school's ICT facilities: 13
Exceptions from unacceptable use: 14
School Social media accounts 15
Monitoring of school network and use of ICT facilities 15
Student's unacceptable use of ICT and the internet outside of school 16
Data Security 16
Software updates, firewalls, and anti-virus software 16
Data protection 17
Access to facilities and materials 17
Encryption 17
Internet access and filtering 18
Part 2 – Security & Passwords 19
Password Creation guidelines 20
Part 3 – Online Safety 22
Educating parents about online safety and social media 24

Cyber-bullying 24
Preventing and addressing cyber-bullying 24
Examining electronic devices 25
Staff and Social Media 26
Part 4 – Mobile Phone use 28
Staff personal mobile phones 28
Data protection 29
Safeguarding 29
Using personal mobiles for work purposes 29
Sanctions 30
Student's personal mobile phone 30
Sanctions 30
Use of mobile phones by parents, volunteers and visitors 32
Loss, theft or damage 32
Part 5 – School Email 34
Part 6 – Remote Learning 35
Teachers 35
Senior leaders 36
Designated safeguarding lead 36
Pupils and parents 37
Governing board 37
Data protection during Remote Learning 37
Keeping devices secure 38
Monitoring and review 38
Appendix A - Staff Social Media Guidance 40
Appendix 1 Student ICT Acceptable Use Agreement 42
Appendix 2 Staff ICT Acceptable Use Agreement 44
Appendix 3 BYOD Agreement 45

Contacts List

ROLE	NAME	CONTACT DETAILS
Head teacher	Caroline Cook	caroline.cook@thelevelsschool.co.uk
Proprietor	Gian Floris	gian.floris@thelevelsschool.co.uk
Designated Safeguarding Lead (DSL)	Ben Bridger	ben.bridger@thelevelsschool.co.uk
Chair of Governors	Geraldine O Sullivan	Geraldine.osullivan@thelevelsschool.co.uk
ICT Support and Network Management	Colin Macpherson	support@fpmit.co.uk and it@thelevelsschool.co.uk

Rationale

The Levels School's electronic communications systems, assistive technology and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

The use of technology provides a positive tool for learning at The Levels School. We recognise however that the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding. In order to protect against these issues, this policy serves to outline steps taken to keep our students safe in the digital world.

This policy outlines the standards that the school requires all users of these systems to observe, the circumstances in which the school will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the school of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's **Data Protection** Policy for further information. The school is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the school's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's **Staff Code of Conduct** disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The school has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, social media and other forms of on-line communications, internet connection, telephones,

mobile device tablets, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Equality Act 2010
- The Education and Inspections Act 2006
- Freedom of Information Act 2000
- Keeping Children Safe in Education 2026
- cyber-bullying: advice for Head teachers and school staff
- protecting children from radicalisation
- Preventing and tackling bullying
- Relationships and sex education
- Searching, screening and confiscation: advice for schools
- Teaching online safety in schools

Definitions

For ease of use the following terms will be used throughout the policy:

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

"Mobile Digital Device": Any digital storage device that is carried which may have access to the internet.

"Personal use": any use or activity not directly related to the users' employment, study or purpose.

"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2: Staff ICT Agreement).

The Head teacher

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The ICT & Network Manager

The role of the ICT and network manager (FPMIT) within school covers:

- Allocating and monitoring student log-ins.
- Allocating student and staff emails.
- Monitoring use of school internet system and permissions for file access.

- Ensuring that any online safety incidents are logged (through the DSL) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with, via the DSL in line with the school **Anti-Bullying** policy, **Relational** policy and **Exclusion** policy.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our **Safeguarding** policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (using the school Management Information System) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school **Anti-bullying and Relational** policies.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Head teacher and/or governing board.

This list is not intended to be exhaustive.

The ICT Development and Strategy manager

- The individuals responsible for the ICT Strategy and Development at The Levels School is the Proprietor **Gian Floris,** overseen by the **Governing body.** Coordinating with the Head teacher (**Caroline Cook**), ICT Support and Network Manager (**Colin Macpherson**) and necessary staff on the development and implementation of the ICT provision at school.
- The management of appropriate filtering and monitoring systems, as overseen by the DSL (**Ben Bridger**) which are updated on a regular basis and keep pupils safe

from potentially harmful and inappropriate content and contact online while at school, including pornography, terrorist and extremist material.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2) and ensuring that pupils follow the school's terms on acceptable use (Appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged (through MIS) and dealt with appropriately in line with the schools **Relational and Exclusion** policies.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the schools **Anti-bullying, Relational** and **Exclusion** policies.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Head teacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1).

- Apply by the use of mobile devices and photography restrictions as found on Page 27 of this policy ("Use of Mobile Phones by Parents, Volunteers and Visitors").
- Alert school should any concerns or issues arise around use of technology at home.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Students

Students are expected to comply by the rules within this policy, as delivered to them through tutor sessions, assemblies PSHE and ICT lessons, and maintain the expected standards of physical and digital interactions. Every student at the Levels School must fill out the ICT Acceptable Use agreement at the end of this policy (**Appendix 1 – Student Acceptable ICT Use Agreement**).

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, upon arrival, and expected to read and follow the Appropriate Use section. If appropriate, they will be expected to sign agreement to the terms on acceptable use (Appendix 2).

ICT Development

The management of ICT at The Levels School is undertaken by the Senior Leadership Team, and Colin Macpherson which will review development across the school termly, ideally preceding scheduled Governor's Meetings. These reviews will be held with the Proprietor (**Gian Floris**), the Head teacher (**Caroline Cook**) and ICT staff. Where necessary the Designated Safeguarding Lead (and/or Deputies) and SENDCo will be involved when pupil welfare and online safety are discussed.

Aims of the ICT Development at The Levels School:

- To create and maintain an ICT provision for staff and students to support teaching, learning, development of assistive technology and administration, making The Levels School a centre of excellence.
- To devise and oversee a whole school ICT strategy which foresees future developments and offers financial budgeting which governors can trust. Financial projections should manage funds appropriately and effectively.
- To be aware of the safeguarding responsibility of the school with regard to ICT and oversee the provision of guidelines for the use of digital technology.
- To prioritise appropriately the way in which ICT developments take place.
- To be responsible for the management of all the implementation and installation of ICT facilities, assistive technology and oversee the School's Bring Your Own Device (BYOD) strategy, supporting the use of personal devices.
- To be representative of the whole school in both prep and senior departments and maintain a whole school view of the development of ICT.
- To offer widespread ICT access and appropriate training to enable staff to be secure, enthusiastic and skilled users, via Microsoft Education Centre, National College.
- To ensure that all staff are encouraged to become confident and regular users of the school's Management Information System (MIS) as an educational tool.
- Wherever possible, have regard to minimising environmental impact and the carbon footprint of ICT.
- To ensure that the school provides information, guidance and support for parents on the use of personal technology as and when appropriate.

Part 1 – Acceptable Use

Guidance for pupils is delivered through ICT lessons, PSHE and therapy sessions supporting use of assistive technology, as well as assemblies and tutor time. Students are made aware of the sanctions for inappropriate use. Following an investigation any incidents of inappropriate use of ICT in school will be actioned in line with the school **Relational** policy.

Staff training in safeguarding and acceptable use of ICT is conducted through INSET and twilight learning sessions, including PREVENT and use of technology (ICT and Assistive) in the classroom.

Visitors working at The Levels School will be provided with guest access to the **The Levels Guest** network (password with DSL and Office) for internet access for email and online storage/streaming where necessary. When signing in at Reception, a copy of the Staff ICT acceptable use agreement (Appendix 2) will be shown, and their signature will be taken as receipt of acknowledgement to that agreement. Visitors who do not have a working role at school will not be allowed access and will be expected to use their own data access via cellular networks.

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see the **Staff Code of Conduct** and schools **Relational** and **Exclusion** policies for reference).

Unacceptable use of the school's ICT facilities:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.

- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel, including but not limited to any USB devices, gaming devices, network sniffers, etc.
- Downloading or setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head teacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use:

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head teacher's discretion.

Requests for said use should be made to the Head teacher in advance, in writing, no later than 2 weeks before its intended use. The school reserves the right to refuse the request.

School Social media accounts

The school has an official Facebook page and Instagram account managed through socialmedia@thelevelsschool.co.uk,

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The social media account managers hold guidelines for what can and cannot be posted on the accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. Monitoring and filtering is done through the Ubiquity Network management system and Smoothwall. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- User activity/access logs.
- Any other electronic communications.

Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Student's unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the **Relational and Exclusion** policy, if a pupil engages in any of the following ***at any time*** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school community.
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

Data Security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. Please see following section for guidance around password creation and use.

Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's **Data Protection** policy.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Network Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Network Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Head teacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT manager.

Internet access and filtering

The school wireless internet connection is secured through Smoothwall filtering system, managed by the ICT Manager and overseen by the DSL (**Ben Bridger**).

In the event of something not being appropriately filtered by Smoothwall, staff should contact the ICT support (it@thelevelsschool.co.uk and Ben.bridger@thelevelsschool.co.uk

Copying in the Proprietor Gian.Floris@thelevelsschool.co.uk immediately.

If the breach was of an inappropriate website for the students present, the Head teacher should also be notified.

All staff and students will have their internet access filtered through Smoothwall and monitored by the Ubiquity Network Management system.

Part 2 – Security & Passwords

Staff and students are provided with ownership of a unique username and password combination. They are given access to a personal documents area and granularly-permissioned communal shared areas. All account security events are logged.

While the school is using the Bring Your Own Device (BYOD) process of working, the BYOD agreement acknowledges that students and their families give permission for monitoring of the student's Office 365 account on their personal device (see Appendix 3).

The Levels School allows students and staff access to our online educational spaces via their personal Microsoft Office 365 account, providing a gamut of learning tools and benefits; for storage, collaboration, document creation and editing which can be accessed from any computer or mobile digital device. Their account will be used to synchronise information between school and personal devices and provide permission to sign into additional education websites without a surplus of additional usernames and passwords.

The ICT/Network manager facilitates access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other mobile digital devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. This log-in and password will never be disclosed to others under any circumstances.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network manager.

All user accounts and content within remains the property of the school, and if intervention or help is required, the password will be reset by the Network Manager.

By signing the Staff ICT Acceptable Use agreement (Appendix 2), staff acknowledge that they will not store passwords, emails, files, images or data with students or staffs personal information on a system or device that is not managed by the school ICT Manager.

Password Creation guidelines

Creation of passwords for The Levels School accounts is managed by the ICT Manager. If any passwords are required to be created by staff and student users of other platforms, to complete school activities, they must follow these guidelines:

- May not contain any of your names or your username.
- A minimum of eight characters, and contain characters from at least three of the following groups:
    - Uppercase letters - A, B, C …
    - Lowercase letters - a, b, c …
    - Numerals - 0, 1,2, 3, 4, 5, 6, 7, 8, 9
    - Symbols - ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /

A strong password is one that is easy for you to remember but difficult to crack by automated guesswork or discern from a previous version of the password. To make your password more secure, some suggestions are:

- Compact a memorable sentence into a word. For example, "I have a rabbit called Dennis who eats Carrots." becomes "IharcDweC."
- Add a memorable date or string of numbers to your favourite word. You should not use your birthday, PIN or telephone number in any password.
- Start or finish with a capital letter or punctuation symbol.
- Invent and follow a convention to cater for regular password changes. Note that this must ensure a more significant change with each version than merely incrementing numbers.

Avoid things which may cause your password to become weak or problematic:

- Avoid complete standalone dictionary words. For example, *Password* is a weak password.
- Your password should be significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3 ...) are not strong.
- Avoid symbols # or @ or " which may not appear reliably on all keyboards.

Part 3 – Online Safety

Pupils at The Levels School are taught about online safety, social media and being a digital citizen as part of the ICT curriculum, PSHE and through the Pastoral tutor system.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools.
- Relationships and sex education and health education in secondary schools.

This new requirement includes aspects about online safety.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of Key Stage 2**, pupils will know:

- 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.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, they will know:

- 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.
- 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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety and social media

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via the website. It is the school's expectation that parents will monitor their child's appropriate and legal use of social media outside of school.

Where necessary online safety and acceptable ICT usage will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head teacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See the school's **Anti-Bullying**, **Relational** and **Exclusion** policies for reference). As stated in our Safeguarding policy, we do not accept any form of bullying at The Levels School. It is not "just banter", "just having a laugh", "part of growing up", or "kids being kids". Abuse is abuse and will not be tolerated.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

In line with our **Anti-Bullying, Relational** and **Exclusion** policies, the school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The pastoral team will provide discussion around cyber-bullying within tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training via the National College online courses.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school **Relational and Exclusion** policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other mobile digital devices, where they believe there is a 'good reason' to do so, unless that content is part of a criminal or safeguarding investigation (see below).

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school **Complaints** procedure.

Staff and Social Media

Staff will not accept friend requests from students or families via personal social media accounts. Staff will be expected to maintain a discrete presence on these platforms and ensure that:

- Display name does not identify you personally or as aa member of staff of the Levels School.
- Profile picture is discrete, professional and/or unidentifiable.
- Privacy settings are checked regularly.
- Care is taken when tagging other members of staff in images or posts.
- Nothing is shared publicly that would not be shared with any of your pupils.
- Personal social media sites are not used during work hours.
- No comments are made about other staff, colleagues or working at The Levels School.
- No profile association is made between the personal social media profile and the school.
- School email is not linked in personal social media accounts.
- Facebook app is uninstalled from mobile phone devices, or Location is switched off as the app can recognise wifi connections and make friend suggestions based on who else uses the same wifi connection.

Staff seeking guidance for managing their personal social media accounts, should check **Appendix A – Staff Social Media Guidance** at the end of this policy.

Part 4 – Mobile Phone use

At the Levels School we recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Through this policy we aim to:

- Promote, and set an example for, safe and responsible phone use.
- Set clear guidelines for the use of mobile phones for pupils, staff, parents and volunteers.
- Support the school's other policies, especially those related to the **Safeguarding** and **Relational and Exclusion** policies**.**

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection.
- Data protection issues.
- Potential for lesson disruption.
- Risk of theft, loss, or damage.
- Appropriate use of technology in the classroom.

It also take guidance from the following government guidelines (Feb 24) Mobile phones in schools - February 2024

Staff personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present, unless there is an emergency. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff workroom).

The Head teacher will decide on a case-by-basis whether to allow for special arrangements. If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

Data protection

Staff may not use their personal mobile phones to process personal data, or any other confidential school information, unless agreed with the Proprietor (**Gian Floris**) and Head teacher (**Caroline Cook**). For further information, please see our **GDPR** policy and the **Part 1 - Acceptable Use** section within this policy.

Safeguarding

The Levels School acknowledges that our provision supports our students and families through social media use, TEAMs meetings and availability through remote learning (see part 6 on Remote Learning). In all events where the above are to happen, staff are to only use their school accounts for email contact and online/virtual meetings and learning sessions.

Staff will refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps. Staff will avoid publicising their personal contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment. There are school phones, tablet and cameras for this purpose.

In the instances where staff must use their mobile phones to access the internet, it will be through their Microsoft Office 365 staff school account and as such will be moderated and monitored by the ICT/Network Manager.

Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations.
- Supervising off-site trips.
- Supervising residential visits.

When supervising residential visits or school trips staff will be allowed to use personal mobile phones to make emergency contact with students and parents. Otherwise, a school mobile will be made available for routine contact for students and parents for normal operation during an educational visit (please see **Educational Visits** policy for further information).

In circumstances where staff have used their personal mobile phone, they will:

- Use their mobile phones in an appropriate and professional manner, in line with our **Staff Code of Conduct.**
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.
- Where necessary, refrain from using their phones to contact parents. If necessary, contact should be made via the school office unless it is an emergency.

Sanctions

Staff that fail to adhere to these procedures may face disciplinary action.

See the school's **Staff Code of Conduct** policy for more information.

Student's personal mobile phone

We understand that students are travelling a distance to school, many in taxis and so will wish to bring their personal mobile phone to school. All phones are to be handed in to Mrs Middleton on the front desk on arrival to school. Students will then collect them at the end of the day. It is not expected that students will need to use their mobile phone during the school day unless there is a clear therapeutic case for them to do so, or they are to attend a school trip. In the event of possible therapeutic need, the Head teacher / Head of Therapy, with the SENCO will make a case-by-case decision and communicate this to Mrs Middleton.

Sanctions

If a child is found to have their phone in school and not handed it in against the expectation outlined above, the phone will be confiscated (covered under sections 91 and 94 of the Education and Inspections Act 2006) and handed into Mrs Middleton and

held there until it is the end of day. Collection of the phone will need to be signed for by the student's adult family member when it is returned.

As per our **Relational and Exclusion** policies, if it is deemed beneficial, a meeting with the student's family member may be conducted within a short period of the confiscation to discuss the potential use of the phone in school and to ensure that home supports the school's policy around mobile phone use by students.

As stated above in **Part 3 – Online Safety**, in the event that it is suspected the student has used their mobile phone in school in a manner which breaches the **Safeguarding** or **Relational and Exclusion** policies, specifically around pornographic imagery, committing an offence or causing personal injury, the Head teacher, DSL, and/or tutor are empowered to search the student's phone under section 91 and 94 of the DfE's guidance on searching, screening and confiscation.

This search will always be made after the phone is confiscated, with at least 2 members of staff present, after notifying the Head teacher of the intended search.

If any content is found to breach the **Safeguarding** or **Relational and Exclusion** policies parameters around child protection, staff must inform the Head teacher immediately and follow the **Safeguarding** policy for reporting a concern.

All logs of reported incident will be made on MyConcern as per the **Safeguarding** policy.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting.
- Threats of violence or assault.
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation.

Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child.
- Using any photographs or recordings for personal use only, and not posting on social media without consent.
- Not using phones in lessons, or when working with pupils.

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school. A copy of the ICT Acceptable Use agreement will be made available for visitors in reception when they sign in for their visitor's lanyards.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. Should the student have permission to have their mobile phone on them during the day, their family must not try to contact their child on his/her personal mobile during the school day.

Loss, theft or damage

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Visitors, students and parents will be made aware of this disclaimer through:

- Notice in school reception and office.
- Student admission form.
- Policy available through school website and for new pupils and parents.

Confiscated phones will be stored in the school office in a secure locked location.

The Levels School accepts that confiscated phones from pupils become the school's responsibility, and thus can be held responsible for loss, theft, or damage in that event.

Lost phones should be returned to either Reception or the staff room. The school will then attempt to contact the owner.

Part 5 – School Email

The school provides each member of staff and each student with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

As stated above in **Part 4 – Mobile Phone use: Safeguarding**, staff will not share their personal email addresses with parents and students and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Latest instructions on encrypting sensitive files can be found through contacting the ICT Network Manager.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the ICT/Network manager immediately and follow our data breach procedure.

Part 6 – Remote Learning

Remote Learning is a tool in The Levels School's pedagogy and is one of many routes we use to support our student's return to full-time education. It is an useful tool for supporting students who are unable to physically attend school due to anxiety or through long-term, illness-related absence.

Within school, all teaching staff are responsible for setting work and where necessary coordinating remote learning sessions with students. Remote learning session dates and times will be logged with the students Tutor, and then the DSL and/or SENCO, as appropriate.

We recognise that the details of delivering remote learning contained within the **Remote Learning** policy will be adjusted as befits our individual students. This will be supported by evidence within the EHCP and through liaison with SENCO, therapists and DSL.

Teachers

When providing remote learning, teachers must be available during normal school opening hours.

If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.

- Keeping in touch with pupils who aren't in school and their parents:
    - If regular contact is required, then it should done through email initially to set up a contact, followed by either phone call or webcam meeting using Microsoft Teams.
    - Emails from parents and pupils should be answered within 24 hours. If it will take longer, staff will send a holding email to acknowledge receipt of the initial contact and an approximate date/time for returning the email.
    - Any complaints or concerns shared by parents and pupils should be treated with the utmost professionalism, forwarding notification of the complaint or concern to a member of the SLT within an hour. Should there be any safeguarding concerns, staff will follow procedures as laid out in the **Safeguarding** policy.

- If a student is failing to complete work regularly, staff should notify SENCO, Head of Therapy and DSL to request advise and flag any potential safeguarding issues.

- Attending virtual meetings with staff, parents and pupils:
  - It is expected that staff will conduct themselves as per the **Staff Code of Conduct** whilst attending virtual meetings, especially around maintaining a professional image.
  - Staff will ensure that locations chosen for virtual meetings will not breach any privacy of theirs and be sensitive to the learning needs of our students (e.g. avoiding areas with background noise, using a blank wall or a calm, static, virtual background).
  - Parents and students will be informed to use blank backgrounds and maintain appropriate dress codes whilst in the virtual meetings.

If teachers are also working in school during a period of remote learning for students, attempts will be made to create a 'normal' school classroom environment for the students attending the remote session, (e.g.: streaming lessons in school to pupils learning remotely).

Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school with regular review meetings across the week which will be focused on monitoring the effectiveness of that remote learning.
- Reaching out for feedback from staff, parents and students.
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations.
- Liaising with the ICT and Network manager to ensure that any ICT concerns are managed appropriately.

Designated safeguarding lead

The DSL is responsible for overseeing the safeguarding considerations during a period of remote learning, coordinating with the Senior Leadership Team on any matters that have arisen or identified areas for concern.

In all other matters the DSL will continue to commit to their role as laid out in the **Safeguarding** policy.

Pupils and parents

Staff can expect pupils learning remotely to:

- Be contactable during the hours of a normal school day, while acknowledging they may not be present in front of that device during the entire time.
- Seek help if they need it, from teachers.
- Alert teachers if they're not able to complete work.

Staff can expect parents with children learning remotely to:

- Make the school aware if their child is sick or otherwise can't complete work, via email within the same day of the inciting incident.
- Seek help from the school if they need it via the school website or through their child's therapist.
- Be respectful when making any complaints or concerns known to staff.

Governing board

The governing board is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible.
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons.

Data protection during Remote Learning

When accessing personal data for remote learning purposes, all staff members will ensure that they follow the GDPR policy and the **Part1 – Acceptable Use** and **Part 3 – Online Safety** sections of this policy, specifically in relation to storing data on personal devices.

In instances where staff personal devices are being used for remote learning, all files, images, data, etc is to be kept online, within the school's Microsoft Office 365 suite of online software, accessed using staff school account log in. No information or data will be

downloaded to personal devices. Any breach of this procedure may be cause for disciplinary action.

Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – as per our password creation guidance in this policy.
- Ensure that Multi Factor Authentication (MFA) is switched on
- Making sure the device is locked if left unattended
- Not sharing the device among family or friends.

The ICT Manager will ensure that the devices remain secure through:

- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- The device is set to lock itself if left inactive for a period of time.
- Installing antivirus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.

Monitoring and review

The school is committed to ensuring that this policy has a positive impact on pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

- Feedback from parents and pupils.
- Feedback from teachers.
- Records of behaviour and safeguarding incidents.
- Relevant advice from the Department for Education, the local authority or other relevant organisations.

The review will be approved at the next Governor's meeting.

Reviewed: C. COOK 12/9/22; Reviewed: C. Cook and Ben Bridger September 2023

Reviewed: C. Cook and Ben Bridger September 2024

Reviewed: C. Cook and Ben Bridger September 2025

Reviewed: C. Cook and Ben Bridger September 2026

Appendix A - Staff Social Media Guidance

Managing your personal social media accounts as a teacher needs a little careful thought so the following guidance is here to support you in managing this.

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this.
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if…

A pupil adds you on social media:

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the Head teacher about what's happening.

A parent adds you on social media:

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school.
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in.

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you:

- **Do not** retaliate or respond in any way.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to Facebook or the relevant social network and ask them to remove it.
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures (as referenced in our **Staff Code of Conduct**, **Relational and Exclusion** policies), are usually sufficient to deal with online incidents.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix 1 Student ICT Acceptable Use Agreement

All users are responsible for the safekeeping of their school credentials. Access to the system must only be made with the user's own account and password.

The user account and content within remains the property of the school, and if intervention or help is required, the password will be reset.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the Digital Use policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Take or use my mobile device in lessons, unless permission has been given to myself and my parents • Take any photos of the school community members without permission of those being photographed • Access any inappropriate websites, also including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile digital device, or mobile phone (where permission is given), into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2 Staff ICT Acceptable Use Agreement

All users are responsible for the safekeeping of their school credentials. Access to the system must only be made with the user's own account and password.

The user account and content within remains the property of the school, and if intervention or help is required, the password will be reset.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I understand that this agreement works alongside the expectations of me as outlined in the Staff Code of Conduct, and as such I may be subject to disciplinary procedures should I breach them. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3 BYOD Agreement

BRING YOUR OWN DEVICE

TERMS, DECLARATION AND AGREEMENT

All personal devices brought into The Levels School, for use in lessons, must be connected to the school systems. Use of a personal device in school for learning requires you to have signed our **Student ICT Acceptable Use agreement**. By signing both, you agree to uphold the rules and guidance of this policy.

The Levels School utilises a PC-centric IT system and as such we reserve the right to refuse a device that cannot operate with Windows networking software.

Where necessary, the connection with the school systems will be made through installing software on the student's personal device. If this software is uninstalled, your access to the systems will be disabled.

In completing connection with the school systems, that device will be managed by the school ICT Network Manager; FPMIT, via the Ubiquity Network Management system and protected via our Smoothwall filtering system.

Monitoring

The school reserves the right to monitor, intercept, review and erase, without further notice, content on the device that is deemed to be in breach of our Student Expectations policy and the terms within this agreement.

This will only be carried out in order to:

- Prevent misuse of the device.
- Ensure compliance with our rules, standards of conduct and policies in force from time to time.

The Levels School reserves the right to:

- Inspect the device for use of any unauthorised applications or software.
- Investigate or resolve any security incident or unauthorised use of school systems.

It is expected that in signing this agreement, you will co-operate with the school to enable such inspection, access and review, including providing passwords or pin numbers where necessary to access the device or relevant applications. A failure to co-operate with the school in this way may will result in sanctions, up to and including expulsion.

Lost or Stolen Devices

In the event of a lost or stolen device, you must report the incident to the main office immediately, where full details will be taken, and attempts will be made to retrieve the item before the end of the school day.

I understand that I will use my own personal information technology device for learning at The Levels School and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained within this agreement.
- I understand that the terms of this agreement will apply to me at all times, during or outside school hours, when I am on the school site.
- I acknowledge and agree that authorised personnel of The Levels School shall have the rights set out here, including but not limited to the right to access, monitor, review and wipe (as the case may be), data contained on my personal device, which I acknowledge may result in inadvertent access to or destruction of my personal data.
- I understand and agree that The Levels School in its discretion may amend or remove this agreement at any time and that I will be bound by the terms of the agreement as amended.

As a student I understand and agree to the conditions set out. I understand that if I breach this agreement then my device may be removed and held in the school office to be collected at the end of the day by my Parent/Guardian. I also understand that I may lose the privilege of bringing my own device into school and possibly face sanctions.

As a Parent/Guardian I understand that my child will be responsible for adhering to this policy. I have read and discussed this policy with my child and they understand the trust and responsibility required in having their own device in school.

SIGNED (STUDENT) SIGNED (PARENT)

PRINTED NAME AND TUTOR GROUP DATE