Bedford Greenacre Independent School

Policy Document

Individual potential unleashed.
Committed to the wellbeing of every child.

E-Safety and Acceptable Use Policy

This policy also applies to EYFS pupils and children in our Nursery Provision

This policy provides clear guidance on the use of mobile electronic devices in school by staff and pupils to ensure the safety and welfare of the pupils attending our school. Staff, parents and visitors are included.

The school ensures that staff remain vigilant at all times and challenge any signs of child-on-child abuse.

Development / Monitoring / Review of this Policy

This E-Safety and Acceptable Use policy has been developed by the E-Learning Team.

Schedule for Development / Monitoring / Review

This E-Safety and Acceptable Use policy was approved by the Governing Body in:	Spring Term 2024
The implementation of this E-Safety and Acceptable Use policy will be monitored by the:	Designated Safeguarding Lead Deputy Designated Safeguarding Lead E-Learning Team Safeguarding Governor
Monitoring will take place at regular intervals:	Every year
The Governing Body will receive a report on the implementation of the E-Safety and Acceptable Use policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals. This will include reviewing filtering systems.	Every year
The E-Safety and Acceptable Use policy will be reviewed biennially or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Spring Term 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Principal LADO Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering

This policy is consistent with:

- *Keeping Children Safe in Education-Statutory Guidance for Schoolsand Colleges,* September 2025
- *Prevent Duty Guidance,* 2023
- *The use of social media for online radicalisation,* July 2015
- *Preventing and tackling bullying: Advice for Headteachers, staff and governing bodies, DfE July 2017*
- *Teaching Online safety in School,* DfE June 2023
- *Cyberbullying: Advice for Headteachers and school staff* (2014)
- *Advice for parents and carers on cyberbullying* (2014)

Scope of the Policy

This policy applies to all members of the Bedford Greenacre Independent School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's digital technology systems, both in and out of school.

The Education and Inspections Act 2006 empowers our Principal to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Bedford Greenacre Independent School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of Bedford Greenacre Independent School, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. Further clarification can be found from the Department for Education guidance: Searching, Screening and Confiscation (January 2022). This is in-line with our Behaviour Policy.

Bedford Greenacre Independent School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Bedford Greenacre Independent School:

Governors

Governors are responsible for the approval of the E-Safety and Acceptable Use policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving updates and reports about online safety. The E-Safety Governor's role includes:

- regular meetings with the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead
- receiving reports which include:
    - overview of online safety incident logs
    - reviews of the effectiveness of the filtering and monitoring systems.

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school's community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead.
- The Principal and Designated Safeguarding Lead/Deputy Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart in Appendix 2).
- The Principal is responsible for ensuring that the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive updates from the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead as and when appropriate.

Designated Safeguarding Lead/Deputy Designated Safeguarding Lead

The Designated Safeguarding Lead/Deputy Designated Safeguarding Lead has day-to-day responsibility for Online Safety. They should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

The role of the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead roleincludes:

- leading the E-Learning Team
- taking day-to-day responsibility for online safety issues and having a leading role in establishing and reviewing the school's E-Safety and Acceptable Use policy
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- providing training and advice for staff
- liaising with the Local Authority
- liaising with the school's IT Technician (network manager)
- receiving logs and reports of online safety incidents to inform future online safety developments
- meeting regularly with the E-Safety Governor to discuss current issues and update the E-Safety Governor
- attending relevant Governor meetings
- reporting regularly to the Senior Leadership Team

IT Technician

The IT Technician (network manager) is responsible for ensuring:

- that Bedford Greenacre Independent School's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection procedure
- that logs and reports of online safety incidents are created and monitored
- that logs of requests to remove specific sites from filtered lists are maintained

- the filtering systems are applied and updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Designated Safeguarding Lead/Deputy Designated Safeguarding Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school's E-Safety and Acceptable Use policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Principal / Designated Safeguarding Lead/Deputy Designated Safeguarding Lead for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety and Acceptable Use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

E-Learning Team

The E-Learning Team provides a consultative group that has wide representation from the school's community, with responsibility for issues regarding e-learning and online safety and the monitoring of the E-Safety and Acceptable Use policy including the impact of initiatives.

Members of the E-Learning Team will assist the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead with:

- the production / review / monitoring of the school's E-Safety and Acceptable Use policy
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and pupils about the online safety provision
- monitoring improvement actions identified through self-review

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Separate age-appropriate Pupil Acceptable Use Agreements are used as follows:
    - Reception / KS1
    - KS2- KS4
    - Sixth Form
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to know and understand the school's Mobile Electronic Devices policy and Anti-Bullying policy

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Bedford Greenacre Independent School's E- Safety and Acceptable Use policy covers their actions out of school, if related to their membership of the school

The acceptable Use of AI is outlined in our Pupils Acceptable Use Agreements.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Bedford Greenacre Independent School will take every opportunity to help parents understand these issues through parents' evenings, letters and website / Learning Platform. In accordance with the Parent / Carer Acceptable Use Agreement, they will be encouraged to support Bedford Greenacre Independent School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line pupil records
- their children's personal devices in school

Governors / Supply Staff / Visitors / Volunteers

Governors / Supply Staff / Visitors / Volunteers who access the school's systems / websites / platforms as part of the wider school's provision will be expected to sign a Governor / Visitor / Volunteer Acceptable Use Agreement before being provided with access to the school's systems.

Education and Training Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is present in all areas of the curriculum and staff reinforce online safety messages across the curriculum.

- Online safety forms part of the ICT/ PSHCE and RSHE curriculum in particular
- Key online safety messages are reinforced as part of a planned programme of assemblies and Form Time / pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Technician (network manager) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents / Carers
Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and maybe unsure about how to respond.

Bedford Greenacre Independent School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

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

- A programme of online safety training is made available to staff. This will be regularly updated and reinforced.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school's E-Safety and Acceptable Use policy.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Designated Safeguarding Lead/Deputy Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety and Acceptable Use policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Designated Safeguarding Lead/Deputy Designated Safeguarding Lead will provide advice / guidance / training to individuals as required.

Governors
Governors should take part in online safety training / awareness sessions, with particular importance for the E-Safety Governor. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association /or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

Bedford Greenacre Independent School are responsible for ensuring that the school's network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Regular reviews and audits of the safety and security of the school's technical systems are carried out
- Servers, wireless systems and cabling are securely located, and physical access is restricted
- All users will have clearly defined access rights to school systems and devices.
- All users (including pupils from Year 1 and above) are provided with a username and secure password by the IT Technician (network manager) who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password periodically. Bedford Greenacre Independent School may also use class log-on and passwords for EYFS / KS1
- The "master / administrator" passwords for the school ICT system, used by IT Technician (network manager) must also be available to the Principal or other nominated senior leader and kept in asecure place (school safe)
- The School Business Manager, on the advice of the IT Technician (network manager) is responsible for ensuring that software license logs are accurateand up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content is filtered. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Our internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- The Designated Safeguarding Lead and Deputy Designated safeguarding Lead regularly monitor the activity of users on theschool technical systems and users are made aware of this in the Acceptable Use Agreement.
- Any actual / potential technical incident / security breach must be reported immediately to the Principal / Designated Safeguarding Lead/Deputy Designated SafeguardingLead.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school's systems and data. These are tested regularly. The school's infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school systems.
- Staff are forbidden from downloading executable files and installing programmes on school devices.
- Removable media (e.g. USB drives) may be used by users on school devices. Pupils can only use these with the express permission of their teacher. We are working towards an encrypted / secure system which will allow staff to work remotely.

Mobile Technologies (including BYOD/BYOT)

Further details can be found in our Bring Your Own Device to School (BYOD) Policy

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to but not limited to this policy, the Safeguarding Children Policy, Behaviour Policy and Anti-Bullying Policy.

Bullying Policy and Codes of Conduct.

The following checklist provides a brief overview of devices and uses which are permitted:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Pupil owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*No Unless authorised*	*Yes*	*No Unless authorised*
Full network access	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Bedford Greenacre Independent School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website or social media or for marketing purposes
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection / GDPR

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Bedford Greenacre Independent School has an appointed Data Protection Officer (DPO). For further details, refer to the school's Data Protection, Information Sharing and Confidentiality Policy.

Communications

This is an area of rapidly developing technologies and uses. Our policy and strict limitations on the use of electronic communications devices is outlined in our Mobile Electronic Communication Devices Policy for Staff and Pupils.

- The official school's email service may be regarded as safe and secure.
- Users must immediately report, to the Principal / Designated Safeguarding Lead/Deputy Designated Safeguarding Lead, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, blogs etc.) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used in EYFS and KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes this policy sets out clear guidance for staff to manage risk and behaviour online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2011 (introduction updated June 2013, latest terminology update December 2021)'.

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render Bedford Greenacre Independent School liable to the injured party

Bedford Greenacre Independent School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training including: acceptable use, social media risks and data protection
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment

Furthermore, staff must ensure that:

- No reference is made in social media to pupils, parents / carers or school staff other than on the official school social media platform
- Personal opinions should not be attributed to Bedford Greenacre Independent School
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, the communication must not be detrimental to the school. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in either school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Bedford Greenacre Independent School permit reasonable and appropriate access to private social media sites, within the limitations set out in our Mobile Electronic Communication Devices Policy.

Bedford Greenacre Independent School's use of social media for professional purposes will be checked regularly by the Principal and E-Learning Team, to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying is banned and will lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in our school's context, either because of the age of the users or the nature of those activities.

Bedford Greenacre Independent School believe that the activities referred to in Appendix 1 would be inappropriate in our school's context and that users should not engage in these activities in / or outside the school when using school equipment or systems. Bedford Greenacre Independent School's policy restricts usage as indicated in Appendix 1.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see Appendix 1).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (in Appendix 2) for responding to online safety incidents and report immediately to the police.

Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- The Principal/Deputy Head and DSL/Deputy DSL will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the device in question as best you can. Any change to its state may hinder a later police investigation.

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

Sanctions

It is more likely that Bedford Greenacre Independent School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as shown in Appendix 3.

Mobile Electronic Communication Devices Policy for Staff and Pupils

This policy provides clear guidance on the use of mobile electronic communication devices in school by staff and pupils to ensure the safety and welfare of the pupils attending our school. Staff, Parents and visitors are included.

Definition:
Mobile electronic communication devices include: mobile phones, smart phones, smart watches, Fitbits, tablet computers and any mobile communication device equipped with photographic, WI-FI, Bluetooth and/or near field communication (NFC) capabilities. This list is for indication purposes and is not exhaustive.

Bedford Greenacre Independent School has a strict no phones policy which includes all mobile electronic communication devices as indicated above.

All pupils MUST therefore leave their phone (or other mobile electronic communication device) with their form teacher at the start of the day and it will be kept in the classroom safe until collection at the end of the school day.

1. *Introduction*

- This policy provides guidance on the appropriate use of personal mobile electronic communication devices by members of staff and pupils.
- Bedford Greenacre Independent School has a clear policy on allowing pupils to bring mobile electronic communication devices into school, and this policy makes explicit reference to electronic communication devices with a camera facility.

2. *Electronic Devices with Camera Facility*

- There is the potential for mobile electronic communication devices with camera facility to be misused in school. They can become an instrument of bullying or harassment directed against pupils and teachers.

3. *Staff Policy*

Staff use of mobile electronic communication devices during their working school day should be:

- Discreet and appropriate e.g. Not in the presence of pupils. Only used in staffroom.
- Mobile electronic communication devices must not be accessed during lesson times or whenever the member of staff is in the presence of children. Members of staff who wear a smart watch should ensure that the Wi-Fi facility and/or data is not enabled during these times The school will not take responsibility for items that are lost or stolen.
- Staff should never contact pupils or parents from their personal mobile electronic communication device or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, a school telephone should be used.
- Staff should never send to, or accept from, colleagues or pupils, texts or imagesthat could be viewed as inappropriate.

With regard to electronic communication devices with camera facility, a member of staffshould never use this to photograph a pupil(s) or allow themselves to be photographedby a pupil(s).

- This guidance should be seen as a safeguard for members of staff and the school.
- Staff should understand that failure to comply with the policy is likely to result in the enforcement of our Whistleblowing policy and associated procedures.

- If a personal emergency occurs staff and helpers are requested to use a school phone,when reasonably possible.
- All staff must ensure that the school has a record of their up-to-date contact details.
- During group outings a designated member of staff will have access to a school mobilephone and the school camera. Staff are permitted to use their own personal mobile electronic communication devices in emergencies.
- No member of staff's personal cameras will be brought into the school.
- School cameras are allowed in the settings. These will be used to record children's achievements and observations for the pupil's assessments.
- The school does not accept liability for any lost or broken device taken on school trips.

Failure to adhere to this policy will result in disciplinary action

4. Parent Policy

- Parents/carers are requested to sign relevant documentation when their child commences school, giving authorisation for us to photograph their child/ren for assessment and observation purposes. If they prefer not to give us their permission, we will respect their wishes.
- Parents should talk to their child about the appropriate use of text messages as they can often be used to bully pupils.
- Parents or other family members are permitted to photograph their children on school events such as sports day and school performances. Parents must not share photos on social media.
- Parents should refrain from contacting their child using the child's mobile device when on school trips. This is important, particularly during residential trips, so that staff can manage any feelings of homesickness; calls from parents can often inflame the situation, so we ask for parental cooperation in this matter.
- In the event of a severe emergency, such as a terrorist attack, please contact the school first, on the emergency number given, prior to trying to call your child using their mobile device, as by doing so, the group could be put at risk.

5. Pupil Policy

- While we fully acknowledge a parent's right to allow their child to bring a mobile electronic communication device to school if they travel to and from school without adult supervision, Bedford Greenacre Independent School discourages pupils from bringing mobile electronic communication devices to school due to the potential issues outlined above.
- When a child needs to bring an electronic communication device into school, this must be handed in to the form teacher at the start of the day and collected at the end of the day. **Electronic communication devices should be clearly marked so that each pupil knows their own device.** Parents are advised that Bedford Greenacre Independent School accept no liability for the loss or damage to electronic communication devices which are brought into the school or school grounds. It is recommended that no expensive electronic communication device should bebrought into school.
- The school accepts no responsibility whatsoever for the loss or damage of any electronic communication device. A form will be signed by parents to inform the school that they have no responsibility whatsoever.
- Where a pupil is found during the school day by a member of staff to be using an electronic communication device or have one in their possession, the device will be confiscated from the pupil, handed to a member of the school office team who will record the name of the pupil and attach it to the device. The School Office will store the mobile electronic communication device. The pupil may collect the device at the end of the school day. A letter will be sent home to the parents requesting that a permission slip be returned the next day. If this practice continues more than three times, then the school will confiscate the device until

an appropriate adult collects the device from a senior teacher.

- If a pupil is found taking photographs or video footage with a mobile electronic communication device of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken according to the school's Behaviour Policy.
- If images of other pupils or teachers have been taken, the electronic communication device will not be returned to the pupil until the pupil, in the presence of a senior teacher, has removed the images.
- Should a pupil be found to be using their electronic communication device inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a mobile electronic communication device into school.
- The school will teach acceptable use of ICT in lessons.
- Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office.
- Pupils should not use mobile electronic communication devices in the after-schoolprovision. Contact with parents should be via the school telephone system only.
- During school trips in the UK and abroad, pupils are permitted to take a mobile device for emergency use only and the need must be assessed on the risk assessment. It is recommended that for trips to theme parks, cities and the European continent, mobile phones should be in possession for emergency use only.
- The device must not be used for texting, phoning without permission or social media purposes.
- Devices may only be used for photography when relevant to the aim of the trip, i.e. taking pictures for use in design technology, art and photography or other subject specific work.
- Staff will provide guidance to pupils about using their device throughout the trip.
- The school does not accept liability for any lost or broken device taken on school trips.
- During a school trip, pupils should only use the telephone on their mobile device in the event of an emergency. Staff should give an emergency contact number to each of the pupils attending the trip. Pupils should not use the mobile device to contact home during the trip; likewise, parents should refrain from contacting their child using the child's mobile device.
- In the event of a severe emergency, such as a terrorist attack, pupils may use their device to contact parents directly when safe to do so.

Pupils are allowed to take mobile electronic communication devices on school trips, in the UK and abroad; however specific rules apply:

- The device must not be used for texting, phoning without staff permission or social media purposes.
- Devices may only be used for photography when relevant to the aim of the trip, i.e. taking pictures for use in design technology, art and photography or other subject specific work. Staff will provide guidance to pupils about using their device throughout the trip. The above text is a repetition of the points above.

6. Visitors

- Visitors are not permitted to use mobile electronic communication devices whilst they are on school premises.
- Workers on site are able to use mobile electronic communication devices to their companies and for personal use but should not take photographs under any circumstances.

7. Sixth Form

- Pupils in the Sixth Form will only be permitted to use mobile electronic communication devices in the Sixth Form designated areas. No use will be permitted around the main school at any time, unless this is specifically for research purposes in the classroom. Sixth Formers must not take photographs of other pupils at any stage around the school.
- When a child turns 18 years of age, they are still required to follow this policy whilst they remain a student at Bedford Greenacre Independent School.

This policy supports the school's Health and Safety, Anti-bullying and Safeguarding Children policies. It has been endorsed by the Governing Body and will be monitored, reviewed andamended as required.

Appendix 1: Use of Mobile Electronic Communication Devices and Digital Photography in EYFS

Children have their photographs taken to provide evidence of their achievements for developmental records and for marketing. Staff, visitors, volunteers and students are not permitted to use their own mobile electronic communication devices to take or record any images of any children for their own records.

Procedures:

Under GDPR 2018, the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school server and computers, which are password protected.

Only school equipment is used to take photographs.

Photographs may be taken during indoor and outdoor play and may be displayed and used in a child's Learning Journey, as part of the child's developmental records for children and parent/carers to share and make contributions.

Sometimes photographs may contain other children in the background.

Personal mobile electronic communication devices belonging to staff or visitors are not to be used when in the presence of EYFS children.

EYFS Staff are not permitted to use recording equipment on their personal mobile electronic communication devices to take photos or videos of EYFS children.

During outings nominated staff will be permitted to have access to an electronic communication device belonging to the school.

All cameras and mobile electronic communication devices are prohibited in the toilet and nappy changing area.

Use of Cameras and Filming Equipment (including mobile phones) by Parents

Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.

Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.

Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.

Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school will always print a reminder in the programme of events where issues of copyright apply.

Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils including in any pupil play spaces, classrooms and/or playgrounds.

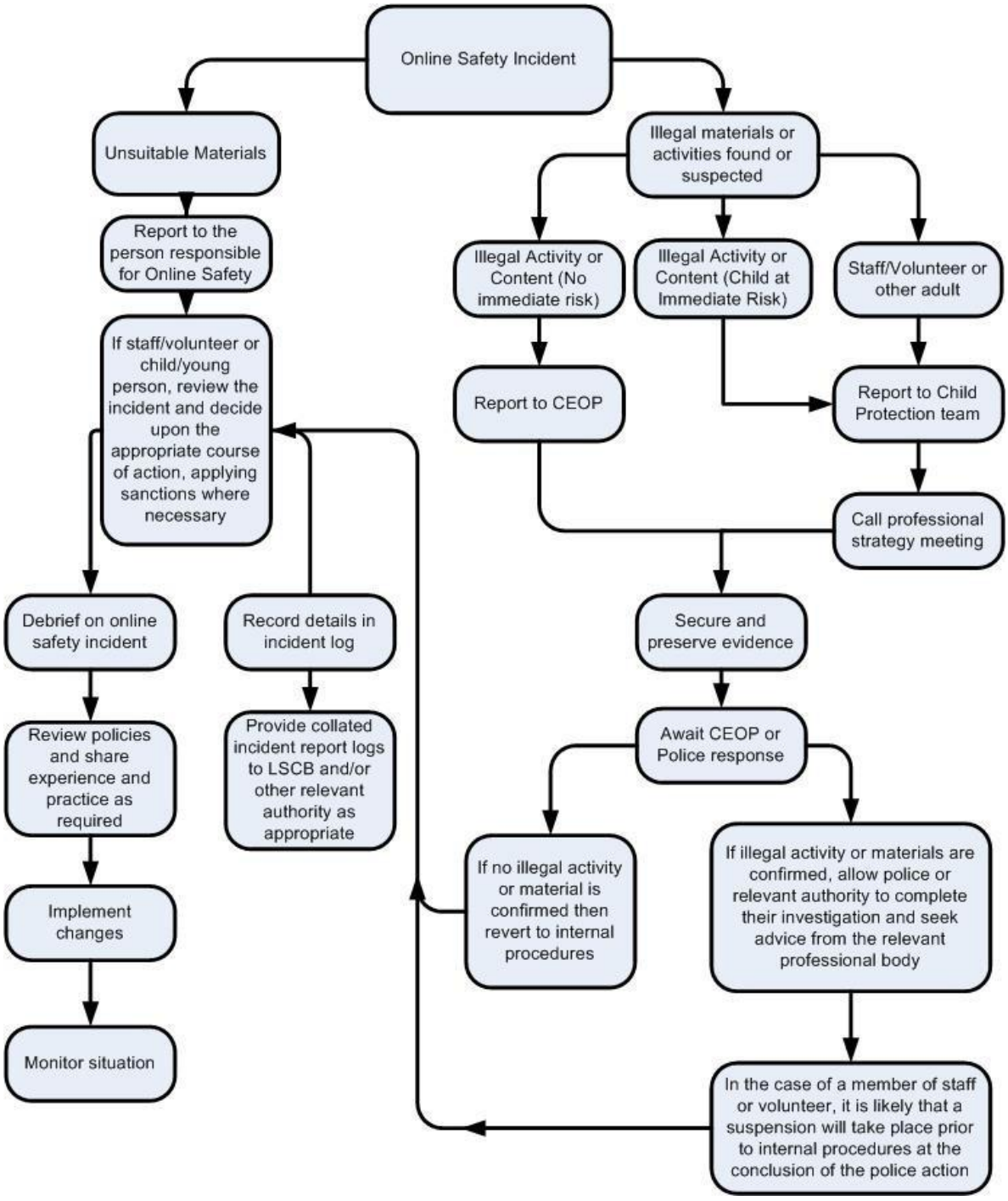
The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

The school sometimes records plays and concerts professionally, in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

Appendix 2: Unsuitable / Inappropriate activities

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school's systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	X
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce				X		
File sharing on school's approved platforms		X				
Use of school's social media		X				
Use of messaging apps						
Use of video broadcasting e.g. YouTube				X		

Appendix 3: Responding to incidents of misuse



Appendix 4: Actions / Sanctions (these lists are not exhaustive)

	Actions / Sanctions								
Pupil Incidents	Refer to class teacher / form tutor	Refer to DSL / Deputy DSL	Refer to Principal	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / Internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal	X	X	X	X		X			X
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised / inappropriate use of any mobile electronic communication device	X					X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X				X			X
Unauthorised downloading or uploading of files	X							X	
Allowing others to access school's network by sharing username and passwords	X					X		X	
Attempting to access or accessing the school, using another pupil's account	X					X		X	
Attempting to access or accessing the school network, using the account of a member of staff	X		X			X			X
Corrupting or destroying the data of other users	X		X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X			X
Using proxy sites, VPNs or other means to subvert the school's filtering system	X		X		X	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act including GDPR	X		X		X	X	X		X

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Principal /DSL	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see Appendix 1).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal Email	X					X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X			X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		X
Deliberate actions to breach data protection or network security rules		X			X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X	X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X						X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X				X		X
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X		X
Using proxy sites, VPNs or other means tosubvert the school filtering system		X					X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
Deliberately accessing or trying to access offensive or pornographic Material		X	X				X	
Breaching copyright or licensing Regulations	X					X		X
Continued infringements of the above, following previous warnings or sanctions		X					X	

Appendix 4a: Form for reporting actual / potential technical incident / security

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse within school. It can be used to inform initial action but is not a substitute for a thorough risk assessment / investigation.

This should be used alongside Appendix 1, Appendix 2 and Appendix 3.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, you must follow the school's Safeguarding Children Policy and procedures, and if necessary, contact the police.

Type of incident: Sexual / Bullying / Violence / Incitement / Financial / Grooming /Other

How was the incident discovered?
Self reported / Reported by 3rd party (friends or parents) / Reported by teacher / Other(e.g. Police or Internet Watch foundation) *

What was their response to the incident?
Unconcerned / Curious / Distressed / Frightened / Secretive / Other

What did the incident refer to?
Answer the key questions relating to the particular incident.

Child as Victim:
Content

1. What was the type of content? (Sexual, violence, racial, other)
2. Did anyone else see it?
3. Have they told anyone else about it?

Publishing

1. Is the child identifiable?
2. Can their location be traced
3. Is text or image potentially indecent or illegal?

Bullying

1. What was the type of bullying? (sexual, violent, physical, group)
2. Were information or images published of the child? (If yes, refer back to publishing section for more questions to ask)

Predation / Grooming

1. Assess the extent of the contact
    - One off conversation
    - Regular conversation
    - Regular conversation using inappropriate or sexualised
    - Language or threats
    - Attempts to breakaway
    - Offline meeting arranged
    - Offline meeting occurred (consider if an offence has occurred)
2. Are the parents aware?
3. When did the incident occur?

Request for information

1. Did the child give out any personal information?

Child as Instigator:
Content
Refer to 'Child as Victim' questions on content

Incitement

1. Was the child secretive about the site?
2. Did the child access the site in an isolated place?
3. Did they understand the risks of accessing this site?
4. Was their response to the site?
    - Healthy (e.g. using for research)
    - Problematic (looking for advice or guidance)
    - Harmful (relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites

Send/Publishing

1. Has an offence taken place? (Refer to glossary for information on what constitutes an offence)
2. Were others put at risk e.g. their image / information was sent / published
3. Was this an isolated incident or persistent?
4. Did the instigator have empathy for the victim?

Document

Interception of communications / Hacking

- Have they placed themselves or others at risk?
- Has personal or financial information been stolen? (If yes, this constitutes a criminal offence, and advice should be sought from the police)
- Has illegal content been accessed and sent to other's computers?

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using existing policies and resources to support children) or in certain circumstances with external help.

Staff misuse

Did the member of staff misuse the school's internal email system?
Did the member of staff communicate with a young person inappropriately e.g. via text message, multimedia images.

Consider the extent of the communication

- One off conversation
- Regular conversation
- Regular conversation using inappropriate or sexualised language or threats
- Attempts to breakaway
- Offline meeting arranged
- Offline meeting occurred (consider if an offence has occurred)

Did the member of staff access inappropriate/ illegal material within school?
Did the member of staff access inappropriate/ illegal material using school equipment?
Did the member of staff access inappropriate/ illegal material using their own equipment?

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, you must follow the school's Safeguarding Children Policy and procedures, and if necessary, contact the police.

BGI school adheres to the KCSIE paragraph 136 regarding content, contact, conduct and commerce. Pupils are educated in these 4 issues

Appendix 5: Audit Tool

The school has an e-Safety Policy that complies with CFE guidance.	
Pupils are aware and sign a Pupil Acceptable Use Agreement.	
The Policy is available for staff on the shared drive and on the school website.	
The Policy is available for parents on the website.	
The Designated Safeguarding Leads are E Brewer, T Djukic, E Niro & T Rodd	
The e-Learning Team members are E Brewer, T Djukic, J Mack, R Woodward & M Sorbo	
Staff undertake E-Safety training every 3 years	
All staff sign an Acceptable Use Agreement on appointment.	
Parents sign and return an Acceptable Use Agreement that their child will comply with the school E-Safety policy.	
Rules for Responsible Use have been set for pupils and are displayed in school. Pupils also sign and return an Acceptable Use Agreement.	
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe andsecure access.	
School personal data is collected, stored and used according to the principles of the Data Protection Act.	
Pupil data is processed in accordance with both Microsoft's and Google's terms and conditions in relation to their school Microsoft and school Google accounts.	