



## **Denefield School**

### **Data protection, e-safety and acceptable use policy**

Approved by Resources on	14 March 2024
Date of next review	March 2025
Review cycle	Annual
Policy control sheet updated	Yes
Type of policy	Statutory
Policy owner	Director of Operations (HML)
Location of policy	Website

# Denefield School

## Data protection, e-safety and acceptable use policy

### Contents

1. Introduction and Aims .....	5
2. Legislation and guidance .....	6
3. Definitions .....	7
4. The data controller .....	8
5. Roles and responsibilities .....	9
5.1 Trust board .....	9
5.2 Data protection officer .....	9
5.3 Headteacher .....	10
5.4 All staff .....	10
5.5 The designated safeguarding lead .....	11
5.6 Director of Operations .....	11
5.7 Parents .....	12
5.9 Students .....	12
5.8 Visitors and members of the community .....	12
6. Data protection principles .....	12
7. Collecting personal data .....	13
7.1 Lawfulness, fairness and transparency .....	13
7.2 Limitation, minimisation and accuracy .....	14
8. Sharing personal data .....	15
9. Subject access requests and other rights of individuals .....	15
9.1 Subject access requests .....	15
9.2 Children and subject access requests .....	16
9.3 Responding to subject access requests .....	17
9.4 Other data protection rights of the individual .....	17
10. Parental requests to see the educational record .....	18
11. Biometric recognition systems .....	18
12. CCTV .....	19
13. Photographs and videos .....	19
14. Data protection by design and default .....	20

15. Data security and storage of records.....	20
16. Disposal of records .....	21
17. Personal data breaches.....	21
18. Educating students about online safety .....	22
19. Educating parents about online safety .....	23
20. Cyber-bullying .....	23
20.1 Definition .....	23
20.2 Preventing and addressing cyber-bullying.....	23
20.3 Examining electronic devices .....	24
21. Acceptable use .....	24
21.1 Staff (including trustees, volunteers, and contractors) access to school ICT facilities and materials.....	25
21.1.1 Use of phones and email .....	25
21.1.2 Personal use .....	26
21.1.3 Personal social media accounts .....	26
21.1.4 Remote access .....	27
21.1.5 School social media accounts.....	27
21.2 Students.....	27
21.3 Parents .....	28
22. Students using mobile devices in school.....	28
23. Staff using work devices outside school.....	29
24. Unacceptable use .....	29
24.1 Exceptions from unacceptable use.....	30
24.2 Sanctions .....	30
24.3 Monitoring of school network and use of ICT facilities .....	30
25. How the school will respond to issues of misuse.....	31
26. Data security.....	31
26.1 Passwords .....	31
26.2 Software updates, firewalls, and anti-virus software.....	32
26.4 Access to facilities and materials.....	32
26.5 Encryption .....	32
26.6 School on premise servers and cloud services .....	33
27. WIFI access .....	33
27.1 Parents and visitors.....	33

28. Training.....	33
29. Monitoring arrangements .....	34
30. Links with other policies .....	34
A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned .....	34
Actions to minimise the impact of data breaches .....	35
Appendix 1: Personal data breach procedure .....	36
Appendix 5: Social Media cheat sheet for staff .....	41
What do to if... .....	42
A student adds you on social media.....	42
A parent adds you on social media.....	42
You're being harassed on social media, or somebody is spreading something offensive about you ...	43
Appendix 6: Flowcharts for managing an eSafety incident.....	43

## 1. Introduction and Aims

ICT is an integral part of the way our school works, and is a critical resource for students, staff, trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

To manage these risks, this policy sets out key organisational aims, as well as rules for staff, visitors, agents and student to comply with. This policy also sets out what is acceptable use and seeks acceptance by all parties involved, including parents to adhere to this policy and to understand the consequences of noncompliance. Data protection aims

Our school aims to ensure that all personal data collected about staff, students, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(EU\) 2016/679 \(GDPR\)](#) and the [Data Protection Act 2018 \(DPA 2018\)](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### E-safety aims

We aim to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate to protect all members of the school community we will:
  - Set guidelines and rules on the use of school ICT resources for staff, students, parents and trustees
  - Establish clear expectations for the way all members of the school community engage with each other online
  - Support the school's policy on safeguarding
  - Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
  - Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including trustees, staff, students, volunteers, contractors and visitors.

#### Acceptable use aims

Our school aims to ensure staff, students, parents, trustees and visitors understand what is deemed acceptable use of the school network, school provided equipment, service or software. Regardless of access method or location. All parties should also understand the consequences of breaching the acceptable use guidelines.

## 2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

This policy reflects the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It refers to the Department's guidance on protecting children from radicalisation.

It also reflects existing legislation, including but not limited to the Education Act 1996, Education and Inspections Act 2006, Equality Act 2010, Education Act 2011, Computer Misuse Act 1990, Human Rights Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Freedom of Information Act 2000. This policy complies with our funding agreement and articles of association.

### 3. Definitions

TERM	DEFINITION
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's: ➤</p> <ul style="list-style-type: none"><li>➤ Name (including initials)</li><li>➤ Identification number</li><li>➤ Location data</li><li>➤ Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data, which is more sensitive and so needs more protection, including information about an individual's: ➤</p> <ul style="list-style-type: none"><li>➤ Racial or ethnic origin</li><li>➤ Political opinions</li><li>➤ Religious or philosophical beliefs</li><li>➤ Trade union membership</li><li>➤ Genetics</li><li>➤ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>➤ Health – physical or mental</li><li>➤ Sex life or sexual orientation</li></ul>
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
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 trustees, staff, students, volunteers, contractors and visitors
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

#### 4. The data controller

Our school processes personal data relating to parents, students, staff, trustees, visitors and others, and therefore is a data controller.

The school is registered with the ICO, as legally required.



## 5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. Relevant sections of this policy also apply to Trustees, Students, Parents, Visitors and Volunteers.

### 5.1 Trust board

The Trust board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The Trust board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Trust 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).

The Resources committee oversees online safety.

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

### 5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description. Our DPO is Paul Hamilton and is contactable via [HML@denefield.org.uk](mailto:HML@denefield.org.uk).

### 5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

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

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

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 3), and ensuring that students follow the school's terms on acceptable use (appendix 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 5.5 The designated safeguarding lead

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
  - Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
  - Ensuring that any online safety incidents are logged (see appendix 5) 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 behaviour policy
  - Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
  - Liaising with other agencies and/or external services if necessary
  - Providing regular reports on online safety in school to the headteacher and/or Trust Board
- This list is not intended to be exhaustive.

### 5.6 Director of Operations

The Director of Operations is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including 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
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

## 5.7 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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 (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the Denefield online safety page - [Denefield School - Online safety](#). They can also get information from the following organisations and websites. Use Google or another search provider to look up:

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

## 5.9 Students

Students are expected to read, understand and agree to the terms on acceptable use of the school's ICT systems and internet (appendix 2)

## 5.8 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date

- Kept for no longer than is necessary for the purposes for which it is processed ➤

Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation

- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

## 7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

## 8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

## 9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.



### 9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

### 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)

- Prevent use of their personal data for direct marketing
- Object to processing which has been justified based on public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement) ➤ Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

#### 10. Parental requests to see the educational record

As an Academy, Denefield is not legally obliged to provide Parents, or those with parental responsibility free access to their child's educational record. (Copies of reports can be requested, or data provided as a Subject Access request. Please see Section 9.

#### 11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners by using a pin number if they wish.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the

relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## 12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Paul Hamilton, Director of Operations.

## 13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

#### 14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply ➤

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

#### 15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Strong passwords used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

## 16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium

- › Safeguarding information being made available to an unauthorised person
- › The theft of a school laptop containing non-encrypted personal data about students

## 18. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

- › 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
- › 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 safe use of social media and the internet will also be covered in other subjects where relevant.

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

#### 19. Educating parents about online safety

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.

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

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

#### 20. Cyber-bullying

##### 20.1 Definition

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 also the school behaviour policy.)

##### 20.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their 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 cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets 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 Anti-bullying and behaviour policies. Where illegal, inappropriate or harmful material has been spread among students, 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.

### 20.3 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 students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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 students 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 students' electronic devices will be dealt with through the school complaints procedure.

### 21. Acceptable use

All students, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 2 and 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.



We will monitor the websites visited by students, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above.

#### 21.1 Staff (including trustees, volunteers, and contractors) access to school ICT facilities and materials

The school's Director of Operations manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other 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.

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 Director of Operations.

##### 21.1.1 Use of phones and email

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

This email account should be used for work purposes only.

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

Staff must 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 must be encrypted so that the information is only accessible by the intended recipient.

Staff must make use of phone or text, not a separate mail (which could be also be intercepted if the account is compromised) to pass on the encryption key to the intended recipient

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 Director of Operations immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students.

#### 21.1.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Director of Operations may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined elsewhere in this policy
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) as long as it does not constitute 'unacceptable use', as defined elsewhere in this policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 5) and use of email to protect themselves online and avoid compromising their professional integrity.

#### 21.1.3 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 5).

#### 21.1.4 Remote access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Director of Operations may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the relevant sections of this policy.

#### 21.1.5 School social media accounts

The school has an official Twitter page, managed by the Director of Operations. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

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

### 21.2 Students

#### 21.2.1 Access to ICT facilities

Computers and equipment in the school are available to students only under the supervision of staff

Sixth-form students can use the computers in the library, workroom and break-out areas independently for educational purposes only.

#### 21.2.2 Unacceptable use of ICT and the internet

The school will sanction students, in line with the behaviour policy if a student 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 students, 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
- 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

## 21.3 Parents

### 21.3.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

### 21.3.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

## 22. Students using mobile devices in school

Students may bring mobile devices to school but are not permitted to use them in the school grounds. Phones brought to school are entirely at the students own risk and that the school cannot take responsibility for lost or damaged items.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

### 23. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Work devices must be used solely for work activities.

### 24. Unacceptable use

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 section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- 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 students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- 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 headteacher or any other relevant member of staff 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.

#### 24.1 Exceptions from unacceptable use

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

#### 24.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's relevant disciplinary policies available on the school website

#### 24.3 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls

- › User activity/access logs
- › Any other electronic communications

Only authorised ICT 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

## 25. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in this policy the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 26. 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, students, parents and others who use the school's ICT facilities must use safe computing practices at all times.

### 26.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action.

Parents or volunteers who disclose account or password information may have their access rights revoked.

#### 26.2 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.

#### 26.3 Data protection

All personal data must be processed and stored in line with data protection regulations and this policy

#### 26.4 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 Director of Operations.

Users must 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 must alert the Director of Operations immediately.

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

#### 26.5 Encryption

The school ensures that relevant 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 student information) out of school if they have been specifically authorised to do so. Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Director of Operations



## 26.6 School on premise servers and cloud services

The school maintains sensitive data on a number of on premise and cloud servers. The security of these servers is paramount.

All on premise servers are in secure rooms with limited access. All server access is protected by strong passwords only known to the Director of Operations and the Schools ICT support partner, RM.

All servers are managed, patched and hardened against vulnerability by our support partner.

All cloud service providers are vetted prior to engagement, to ensure their contractual terms comply with the GDPR and the Data Protection Act 2018.

## 27. WIFI access

The school wireless internet connection is secured.

The school WIFI password is not shared and any devices that need to connect to the WIFI must be given to the ICT technician to do so.

The school always uses strict internet and email filtering. If you feel something has been filtered in error or should not have passed the filter, please report it to the Director of Operations.

### 27.1 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's WIFI unless specific authorisation is granted by the Director of Operations.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g., as a volunteer or as a member of the PTA)
- Visitors need to access the school's WIFI in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WIFI password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

## 28. Training

All staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 29. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years by the Trust Board's Resources committee.

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

## 30. Links with other policies

The data protection sections of this policy are linked to our:

- Freedom of information publication scheme

The e-safety sections of this policy are linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Privacy notices
- Complaints procedure

A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO

expects to have further information. The DPO will submit the remaining information as soon as possible

➤ The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above, any decision on whether to contact individuals will be documented by the DPO.

➤ The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

➤ The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts relating to the breach
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals) Records of all breaches will be stored by the DPO

➤ The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

#### Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

#### Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the school DPO.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - other categories and approximate number of individuals concerned
    - the categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach

## Appendix 2: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement 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:
- Access any inappropriate websites 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 phone or other personal electronic device into school:
- I will not use it within the school grounds

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 (student):

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 students 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 3: acceptable use agreement (staff, trustees, volunteers and visitors)

#### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/trustee/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 students without checking with teachers first
- Share confidential information about the school, its students 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 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 student 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 students in my care do so too.

Signed (staff member/trustee/volunteer/visitor):

Date:

#### Appendix 4: online safety incident report log

##### ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident



--	--	--	--	--

## Appendix 5: Social Media cheat sheet for staff

Don't accept friend requests from students on social media

### 10 rules for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling social media apps from your phone. The apps recognise wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or students)

## Check your privacy settings

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, students 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](https://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](https://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 do to if...

### A student adds you on social media

In the first instance, ignore and delete the request. Block the student from viewing your profile. Check your privacy settings again, and consider changing your display name or profile picture

If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher 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

Students 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 the relevant social network and ask them to remove it

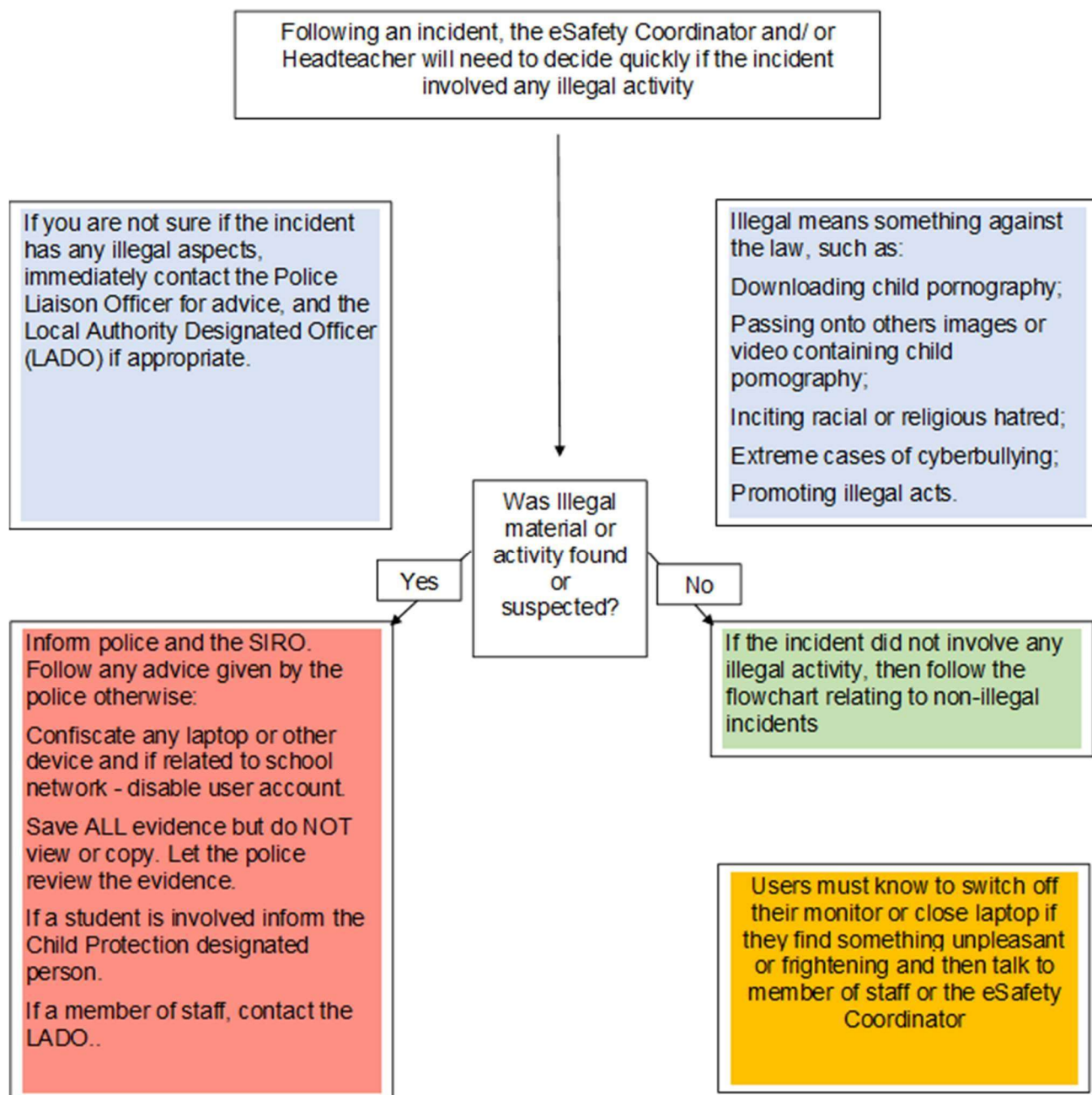
If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

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 6: Flowcharts for managing an eSafety incident

Flowchart to support decisions related to an illegal eSafety incident



Flowchart to support decisions relating to other eSafety incidents

If the incident **did not** involve any **illegal activity**, then follow this flowchart

**The eSafety coordinator and/or Headteacher should:**

Record in the school eSafety Incident Log

Keep any evidence

If member of staff has deliberately or accidentally:

behaved in a way that has harmed a child, or may have harmed a child;

possibly committed a criminal offence against or related to a child or

behaved towards a child or

children in a way that indicates he

or she would pose a risk of harm if

they work regularly or closely with

children, contact the LADO

If the incident does not satisfy the school criteria, then follow the points below:

Review evidence and determine if the incident is accidental or deliberate;

Decide upon the appropriate course of action;

Follow school disciplinary procedures (if deliberate) and contact school HR

Incident could be:

Using another person's username and password without permission of Head Teacher

Accessing websites which are against school policy e.g.:

Using a mobile phone to make a sound or video recording during a lesson;

Using the technology to upset or bully (in extreme cases could be illegal)

Did the incident involve a member of staff?

Yes

Was the child the victim or instigator?

Victim

Instigator

In-school action to support student by one or more of the following:

class teacher

eSafety Coordinator

senior leader or Headteacher

designated senior person for child protection

Inform parents/carers as appropriate. If the child is at risk inform the CPO immediately.

Confiscate the device, if appropriate.

Review incident and identify if other students were involved

Decide appropriate sanctions and/or support based on school rules/guidelines

Inform parents/carers –unless informed by social services and/or police that parental contact is not appropriate

In serious incidents consider informing the CPO as the child instigator could be at risk.

Review school procedures/policies to develop best practice.

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator



**All incidents should be reported to the Headteacher, Designated safeguarding officer or Trustees who will:**

Record in the school eSafety Incident Log;

Keep a written form of evidence for incidents and where the incident is related to images/screen shots describe the evidence in words and record website address without accessing or saving the images in question

Use the 'Report Abuse' button if appropriate or available

Reporting the incident to the Trustees.

Parents/carers as instigators - follow some of the steps below:

Contact the person and invite into school and discuss using some of the examples below:

You have become aware of discussions taking place online;

You want to discuss this

You have an open-door policy so disappointed they did not approach you first;

They have signed the Home School agreement;

Request the offending material be removed

If this does not solve the problem, consider involving the Chair of Trustees.

Staff as instigators - follow some of the steps below:

Contact School HR for initial advice and/or contact the eSafety coordinator;

Contact the member so staff and request the offending material be removed immediately, in serious cases you may be advised not to discuss the incident with the staff member;

Refer to the signed ICT Acceptable Use Agreement and consider if this incident has an impact on the Contract of Employment of the member of staff.

Students as instigators - follow some of the steps below:

Identify the students involved;

Ask student to remove offensive material. Refer to signed Acceptable Use Agreement.

If the perpetrator refused to remove the material and is under 13, contact the Social Network who will close the account.

Take appropriate actions in-line with school policies/rules.

Inform parents/carers unless informed by social services and/or police that parental contact is not appropriate

if the child is at risk talk to your school Child Protection designated person

Further contacts to support staff include:

School eSafety adviser

School HR

School Governance

Local Police

LA legal team helpline

The Headteacher or Chair of Trustees can be the single point of contact to coordinate responses.

The members of staff may also wish to take advice from their union.

For serious incidents or further advice:

Inform your local police neighbourhood team;