RIPPLEVALE

SCHOOL

Data Protection (UK GDPR) Policy

Staff Responsible:	DPO/Senior Administrator	
Approved by:	Jane Norris	**Date:** 03/09/2018
Last reviewed on:	March 2022	
Next review due by:	March 2023	

Ripplevale School
Data Protection (UK GDPR) Policy (March 2022)

‘Ripplevale School provides a caring, learning environment where our students make meaningful progress, relative to their individual starting points. Our aim is to encourage them to develop appropriate personal, social and employable skills enabling them to become confident, independent and aspiring young people.’

This policy was updated in March 2022. The majority of changes made add consistency to spelling, style and formatting conventions. There have been some changes to the content of the policy. All changes (additions, revisions and/or removals) have been indicated by the use of this grey font to highlight changed or new material. The main additions relate to:

- Inclusion of references to the School’s Data Protection Officer (GPO)
- Inclusion of references to the UK GDPR (which has replaced the European GDPR)

1 Purpose

To function effectively Ripplevale School [the School] needs to collect and use certain types of information about staff, students and other individuals who come into contact with the School. We are also obliged to collect and use data to fulfil our obligations to Local Education Authorities, the Department for Education and other professional bodies.

We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats personal information lawfully and correctly. To this end we fully endorse and adhere to the principles of data protection as detailed in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

You should be aware that, under the Act and UK GDPR, you are personally accountable for your actions and can be held criminally liable if you knowingly, or recklessly, breach it. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under the School’s disciplinary procedures. If you access another employee’s personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

2 The data protection principles

There are data protection principles that are central to the Act and UK GDPR. The School and all its

employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act/UK GDPR. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

    - health
    - race or ethnic origin
    - political opinions and trade union membership
    - religious or other beliefs
    - physical or mental health or condition
    - sexual life or sexual orientation
    - genetic and biometric data (new to UK GDPR)

    Criminal data has separate rules under UK GDPR but is still dealt with as sensitive.

2. The lawful purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

3. "Adequate, relevant and not excessive." The School will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is sound business reasons requiring information to continue to be held.

4. "Accurate and kept up-to-date." If your personal information changes, for example you change address, you must inform the office as soon as practicable so that the School's records can be updated. The School cannot be held responsible for any errors unless you have notified us of the relevant change.

5. "Not kept for longer than is necessary." The School will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the School decides it does not need to hold for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of six months.

6. Personal data processed for any of the lawful purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage). Personnel files are confidential and are stored in a secure office in a locked cupboard. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked

drawers when not in use by authorised employees. Data held on computers will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. The School has network backup procedures to ensure that data on computers cannot be accidentally lost or destroyed.

3 Your consent to personal information being held

The School holds personal data about you. By signing your statement of main terms of employment and your job description (both these documents form your contract of employment), you have consented to that data being processed by the School for any purpose related to your continuing employment or its termination including, but not limited to, payroll, human resources and School continuity planning purposes. Agreement to the School processing your personal data is a condition of your employment. This includes giving your consent to the School using your name and maybe your photograph in its marketing or promotional material, whether in hard copy print format or online on the School's website. It also includes supplying the School with any personal data that it may request from you from time to time as necessary for the performance of your contract of employment and for continuity of employment, such as DBS checks.

The School holds limited sensitive personal data about its employees and, by signing your contract of employment, you give your explicit consent to the School holding and processing that data, for example sickness absence records, health needs and equal opportunities monitoring data.

4 Your right to access personal information

You have the right, on request, to receive a copy of the personal information that the School holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You also have the right on request to:

- Be told by the School whether and for what purpose personal data about you is being processed
- Be given a description of the data and the recipients to whom it may be disclosed
- Have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- Be informed of the logic involved in computerised decision-making

Upon request, the School will provide you with a statement regarding the personal data held about you. It will state all the types of personal data it holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request for this.

If you wish to make a complaint that these rules are not being followed in respect of personal data the School holds about you, you should raise the matter with the Data Protection Officer (DPO): Dave Parsons.

If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under the School's grievance procedure.

5 Your obligations in relation to personal information

If, as part of your job duties and responsibilities, you collect personal information about employees or other people such as students, volunteers, work experience placements, consultants or School visitors, you must comply with this policy. This includes ensuring the information is processed in accordance with the Act/UK GDPR, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary. You must also comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject. In particular, it should not be:

    1. Given to someone from the same family.
    2. Passed to any other unauthorised third party.
    3. Placed on the School's website.
    4. Posted on the Internet in any form.

Unless the data subject has given their explicit prior written consent to this

Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone, this is particularly important with student information and if in doubt in regard to student information, DO NOT give information out, refer to Designated Safeguard Lead (DSL), and if it is information being requested for a Child in Care (CIC), strictly refer the matter to the Local Authority Designated Officer (LADO).

Where the School provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the School's requirements in this regard.

Only transmit personal information between locations by e-mail if a secure network is in place, for example, an encryption or password is used for e-mail.

If you receive a request for personal information about another employee, you should forward this to the Headteacher who is responsible for dealing with such requests.

This policy will be included in the staff handbook

5 Procedure

5.1 Compliance

The School will comply with the terms of the 2018 Data Protection Act (UK GDPR), and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

5.2 *Online Safety Policy*

This policy should be used in conjunction with the School's *Online Safety Policy*.

5.3 Data gathering

5.3.1. Coverage

All personal data relating to staff, students or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act/UK GDPR.

5.3.2. Relevance

Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

5.4 Data storage

5.4.1 Security

Personal data will be stored in a secure and safe manner.

5.4.2 Electronic data security

Electronic data will be protected by standard password and firewall systems operated by the School.

5.4.3 Visibility

Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception.

5.4.4 Analogue data

"Analogue" (i.e. non-digital) data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

5.4.5 Sensitive data

Particular attention will be paid to the need for security of sensitive personal data.

5.5 Data checking

5.5.1 Reminders

The School will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

5.5.2 Errors

Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

5.6 Data disclosures

5.6.1 Consent

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

5.6.2 Telephone requests

When requests to disclose personal data are received by telephone, it is the responsibility of the School to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimized.

5.6.3 Personal requests

If a personal request is made for personal data to be disclosed, it is again the responsibility of the School to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

5.6.4 Student requests

Requests from parents or children and young people for printed lists of the names of children and young people in particular classes, which are frequently sought at Christmas, should politely refused as permission would be needed from all the data subjects contained in the list.

5.6.5 Personal data in public media

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

5.6.6 Avoiding repetitive requests

Routine consent issues will be incorporated into the School's student data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the School.

5.6.7 Disclosures to Police

Personal data will only be disclosed to Police Officers if they are able to supply the relevant form which notifies of a specific, legitimate need to have access to specific personal data.

5.6.8 Record keeping

A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

5.7 Subject Access Requests

5.7.1 Written requests

If the School receives a written request from a data subject to see any or all personal data that the School holds about them, this should be treated as a Subject Access Request and the School will respond within the 40-day deadline.

5.7.2 Informal requests

Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the School will comply with its duty to respond within the 40-day time limit.

5.8 Policy distribution

This policy will be included in the *Policies Folder*.

5.9 School prospectus

Data protection statements will be included in the School prospectus and on any forms that are used to collect personal data.